DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA SISELCOM S.A.S. BAJO LA NORMA ISO 27001:2013

LADY JOHANA ORDOÑEZ ARIZA
JOSÉ MAURICIO CASTRO GAITÁN

UNIVERSIDAD PILOTO DE COLOMBIA
DIRECCIÓN DE POSTGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA SISELCOM S.A.S. BAJO LA NORMA ISO 27001:2013

LADY JOHANA ORDOÑEZ ARIZA
JOSÉ MAURICIO CASTRO GAITÁN

Trabajo de Grado para optar el título de
Especialista en Seguridad Informática

Asesor:
Jenny Alejandra Varela Segura
MSC en Redes Corporativas e Integración de Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
DIRECCIÓN DE POSTGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

Notas de aceptación:

_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma primer jurado

_____
Firma segundo jurado

Bogotá D.C., Diciembre 2017

DEDICATORIA

Dedico este trabajo a Dios, por darme la oportunidad de vivir y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mis hijos Juan David y Emma Gabriela, quienes alientan cada día para levantarme y luchar hasta el final.

A mi esposa Ángela Milena por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles. A mis padres Efraín y Carmen, por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles

José Mauricio Castro Gaitán

Este logro se lo dedico primero a Dios y a mi familia por todo su apoyo constante, en especial a mi esposo Juan Quiroga quien me motiva a ser mejor cada día, a mí mamá Nelly Ariza y mi hermano Wilder Ordoñez quienes me ayudaron a crecer como una persona íntegra y a mi papá Rafael Ordoñez quien con su ejemplo me inspira a ser mejor cada día.

Lady Johana Ordoñez Ariza

AGRADECIMIENTOS

Le doy especial tributo de agradecimiento a todas y cada una de las personas que contribuyeron con la realización y desarrollo del presente proyecto de grado.

En primer lugar, dar gracias a Dios, el dador de todas las cosas y quien permite que todo ocurra, por permitirnos llegar a este momento. A mis hijos Juan David y Emma Gabriela, quienes alientan cada día para levantarme y luchar hasta el final.

A mi esposa Ángela Milena por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles. A mis padres Efraín y Carmen, por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles

Finalmente, a cada una de las personas que hicieron de nuestra formación lo más grato posible y aún más cada uno de los que intervinieron en este proyecto. Hoy les podemos decir muchas gracias por su mano y apoyo.

José Mauricio Castro Gaitán

Agradezco a mi familia en especial a mi esposo por todo su apoyo, a la universidad por permitirme crecer tanto profesional como personalmente, a todos los profesores que participaron en nuestra formación en especial a nuestra tutora por sus consejos y guía que fueron muy importantes en la culminación del proyecto.

A SISELCOM S.A.S y su gerente Fernando Muñoz por darnos la oportunidad de desarrollar este proyecto dándonos todas las herramientas para lograrlo.

Lady Johana Ordoñez Ariza

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: "cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa información y tiene valor para la organización, como bases de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la empresa"[1].

ACTIVO: "el activo son los bienes, derechos y otros recursos de los que dispone una empresa, pudiendo ser, por ejemplo, muebles, construcciones, equipos informáticos o derechos de cobro por servicios prestados o venta de bienes a clientes. También, se incluirían aquellos de los que se espera obtener un beneficio económico en el futuro"[2].

AMENAZA: "en tecnología son aquellos factores externos que están fuera de nuestro control y que podrían perjudicar y / o limitar el desarrollo de la organización. Las amenazas son hechos ocurridos en el entorno que representan riesgos para la Entidad"[3].

ANÁLISIS DE RIESGOS: "método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado"[4].

CONFIDENCIALIDAD: la propiedad que un activo esté disponible y no sea divulgado a personas, entidades o procesos no autorizados.

CONTROL: en tecnología son las acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía. "Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en

[1] ANGE, Camilo. ¿Qué es un activo de información?. [en línea]. Bogotá: Wordpress, 2010 [fecha de consulta: 15 de octubre de 2017]. Disponible en: https://camiloangel.wordpress.com/2010/09/03/%c2%bfque-es-un-activo-de-informacion/

[2] REVISO. ¿Qué es un activo?. [en línea]. Bogotá: Reviso, 2016 [fecha de consulta: 15 de octubre de 2017]. Disponible en: https://www.reviso.com/es/que-es-un-activo

[3] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN. Glosario. [en línea]. Bogotá: Ministerio de las TIC, 2015 [fecha de consulta: 15 de octubre de 2017]. Disponible en: www.mintic.gov.co/gestionti/615/articles-6099_recurso_2.docx › General

[4] GUTIÉRREZ AMAYA, Camilo. Análisis de riesgos. [en línea]. Buenos Aires: Welive Security, 2012 [fecha de consulta: 15 de octubre de 2017]. Disponible en: www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal"[5].

ESTIMACIÓN DE RIESGOS: proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

EVALUACIÓN DE RIESGOS: proceso global de identificación, análisis y estimación de riesgos.

IMPACTO: el costo para la empresa de un incidente (de la escala que sea), que puede o no ser medido en términos estrictamente financieros, ejemplo, pérdida de reputación, implicaciones legales, etc.

POLÍTICA DE SEGURIDAD: "documento en el cual se estipulan las políticas con respecto a la seguridad de la información de la organización"[6].

POLÍTICA: "arte o traza con que se conduce un asunto o se emplean los medios para alcanzar un fin determinado. Declaración de los principios que presenta la posición de la administración para un área de control definida"[7].

TRATAMIENTO DEL RIESGO: "proceso de selección e implementación de medidas para modificar el riesgo"[8].

[5] INSTITUTO ESPAÑOL DE ANALISTAS. ¿Qué es control?. [en línea]. Madrid: IEAF, 2013 [fecha de consulta: 15 de octubre de 2017]. Disponible en: ieaf.es/new/lideres-de.../control-y...riesgos.../1561-que-es-el-control-de-riesgos.html

[6] INSTITUTO CARO Y CUERVO. ¿Qué es política de seguridad?. [en línea]. Bogotá: Instituto Caro y Cuerto, 2010 [fecha de consulta: 25 de abril de 2016]. Disponible en: www.caroycuervo.gov.co/ sites/.../POLÍTICA% 20DE%20 SEGURIDAD% 20ICC_0.pdf

[7] CONSEJO SUPERIOR UNIVERSITARIO. Acuerdo 046 (1 de diciembre de 2009). Por el cual se definen y aprueban las políticas de Informática y Comunicaciones que se aplicarán en la Universidad Nacional de Colombia. Bogotá: Universidad Nacional de Colombia, 2009. p. 1

[8] ESCUELA DE ADMINISTRACIÓN, FINANZAS Y TECNOLOGÍA. ¿Qué son medidas de tratamiento. [en línea]. Medellin: EAFIT, 2010 [fecha de consulta: 25 de abril de 2016]. Disponible en: www.eafit.edu.co/.../Nota%20de%20Clase%2010%20Medidas%20de%20Tratamiento

RESUMEN

En el presente artículo se muestra el proceso de diseño del sistema de gestión de seguridad de la información (SGSI) para la empresa SISELCOM S.A.S. con el objetivo de establecer el estado actual de la seguridad de la información en la empresa, de acuerdo a los tres pilares fundamentales de la seguridad (integridad, confidencialidad y disponibilidad).

Este diseño ayudara en el proceso de establecer políticas, procedimientos y controles en relación a los objetivos estratégicos del negocio, brindando una visión general del estado de los sistemas de información y la efectividad de las medidas de seguridad implementadas, lo cual, es fundamental para apoyar la toma de decisiones y las estrategias a seguir. Para realizar este diseño y el levantamiento de la información se realizaron entrevistas con la gerencia, visitas de campo, verificación de inventario, valoración de activos de acuerdo al Anexo B de la norma ISO 27005, validación de controles de acuerdo al Anexo A de la norma ISO 27001:2013 y análisis de riesgo basado en la norma ISO 27001:2013.

INTRODUCCIÓN

Para las organizaciones la información está definida como uno de los activos más valiosos y primordiales, los activos sólo tienen un sentido cuando están disponibles y son utilizados de forma adecuada, íntegra, oportuna, responsable y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

Los administradores y personal de cualquier tipo de empresa y organización independiente de su tamaño y naturaleza deben ser conscientes que la diversidad de amenazas existentes que cada día atentan contra la seguridad y la privacidad de la información, representan un riesgo altamente potencial que, al materializarse, puede acarrear costos económicos, sanciones legales, afectación de su reputación e imagen. Sumando lo anterior a un entorno tecnológico en donde cada día se hace más compleja la administración y el aseguramiento de la información alineándolos a los objetivos y planes estratégicos de la organización.

El presente proyecto que es presentado como opción de grado, busca plantear la base para el diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa SISELCOM S.A.S., teniendo en cuenta para esto el marco de referencia de la norma NTC-ISO-IEC 27001:2013 que proporciona un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de gestión de seguridad de la información en cualquier tipo de organización.

1. PLANTEAMIENTO DEL PROBLEMA

En la sociedad actual se viene presentado un constante cambio y evolución en las tecnologías de la información, lo que hace necesario que cada empresa y/o compañía, cuente con un esquema de seguridad de la información que apoye y apalanque los objetivos estratégicos de la organización.

Un sistema de gestión de seguridad de la información (SGSI), permite establecer políticas, procedimientos y controles en relación a los objetivos estratégicos del negocio, brindando una visión general del estado de los sistemas de información y la efectividad de las medidas de seguridad implementadas, lo cual, es fundamental para apoyar la toma de decisiones y las estrategias a seguir.

Con base en el diagnóstico de la situación problema, la empresa SISELCOM S.A.S., requiere el diseño de un sistema de gestión de seguridad de la información (SGSI) con el objetivo de establecer el estado actual de la seguridad de la información en la empresa, de acuerdo a los tres pilares fundamentales de la seguridad (integridad, confidencialidad y disponibilidad).

De acuerdo a lo anterior, se puede establecer que el problema está relacionado con un inadecuado o inexistente modelo de seguridad de la información, lo que significa que es necesario diseñar un Sistema de Gestión de Seguridad de la Información para la empresa, basado en un estándar de seguridad reconocido a nivel mundial, como lo es la norma NTC-ISO-IEC 27001:2013.

1.1 FORMULACIÓN DEL PROBLEMA

¿De qué manera se pueden identificar los riesgos asociados al estado actual de seguridad de los activos y procesos de información en la empresa SISELCOM S.A.S.?.

2. JUSTIFICACIÓN

La implementación de un sistema de gestión de seguridad de la información (SGSI), basado en un modelo de buenas prácticas de seguridad como es la norma NTC-ISO-IEC 27001:2013, proveerá una visión del nivel existente de las condiciones de oportunidad, gobernabilidad y viabilidad necesarias para que la seguridad de la información apoye y extienda los objetivos estratégicos del negocio. Un modelo de seguridad de la Información, le ayudará a la entidad a medir, cuantificar y mejorar el nivel de cumplimiento de los indicadores que se establecieron para determinar el estado actual de la situación problema.

Establecer un diseño de gestión de seguridad de la información, significa que la empresa tiene un interés en proteger su información y contar con un gobierno de seguridad alineado a las necesidades y objetivos estratégicos del negocio, compuesto por una estructura organizacional y un conjunto coherente de políticas, procesos y procedimientos, con el objetivo de promover una cultura de seguridad en todos los niveles de la empresa. Un sistema de gestión de seguridad de la información le permitirá a la entidad gestionar de manera efectiva los riesgos asociados a la seguridad de la información mediante la identificación de amenazas que puedan llegar a comprometer la integridad, disponibilidad y confidencialidad de sus activos.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información que permita identificar los riesgos asociados al estado actual de seguridad de los activos y procesos de información en la empresa SISELCOM S.A.S. y determinar los controles necesarios para su protección, tomando como referencia la norma NTC-ISO-IEC 27001:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar el levantamiento de información, analizando las necesidades y requerimientos para conocer la situación actual de la empresa SISELCOM S.A.S., con relación a la gestión de seguridad de la información con base a la norma NTC-ISO-IEC 27001:2013.

- Establecer la estructura organizacional, roles y responsabilidades en cuanto a la seguridad de la información.

- Elaborar un análisis de riesgo para todos los procesos de la empresa.

- Definir las políticas, alcance y objetivos del sistema de gestión de seguridad de la información tomando como base la norma NTC-ISO-IEC 27001:2013.

- Establecer los controles necesarios tomando como base la norma NTC-ISO-IEC 27001:2013.

4. MARCO DE REFERENCIA

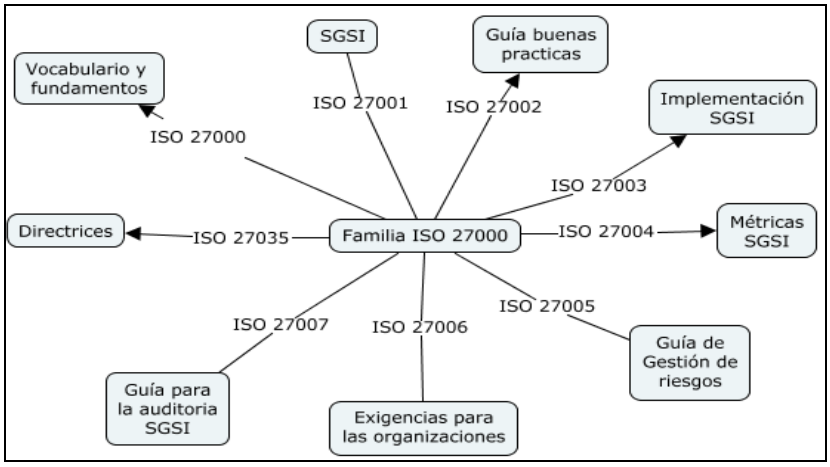
4.1 MARCO TEÓRICO

Con el fin de contextualizar el tema de seguridad de la información y la importancia de la misma y considerando el riesgo latente que existe en las entidades privadas y públicas en Colombia, se indica a continuación algunas definiciones y conceptos básicos que se deben contemplar para la realización de la propuesta:

Dentro de los modelos y normas que pueden ser utilizados para la implementación de un sistema de gestión de la seguridad de la información se encuentra enmarcada la norma ISO/IEC 27001:2013, aprobada y publicada por la ISO - International Organización for standardization. Esta norma proporciona recomendaciones a partir de las mejores prácticas en la gestión de la seguridad de la información, dirigida a todos los responsables de iniciar, implantar o mantener sistemas de gestión de la seguridad (SGSI), partiendo de los conceptos de confidencialidad, integridad y disponibilidad de la información.

La ISO/IEC 27001:2013 hace parte de la familia de normas de la serie ISO/IEC 27000, las cuales contienen mejores prácticas para desarrollar, implementar y mantener especificaciones para los sistemas de gestión de la seguridad de la información (SGSI). La Figura 1 muestra la relación que tiene cada una de las normas que componen la familia 27000:

Figura 1. Familia ISO 27000



Fuente. Los Autores

4.1.1 Compendio de la familia ISO 27000. El compendio de la norma ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por la ISO (international organization for standardization) e IEC (international

electrotechnical commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Este grupo de normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, controlar y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI).

Para Colombia el organismo encargado de normalizar este tipo de normas es el ICONTEC (instituto colombiano de normas técnicas y certificaciones), Entre sus labores se destaca la reproducción de normas técnicas y la certificación de normas de calidad para empresas y actividades profesionales. ICONTEC es "el representante de la Organización Internacional para la Estandarización (ISO), en Colombia"[9].

4.1.1.1 ISO/IEC 27001. Es una norma emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. Además, esta norma establece 114 controles que permiten a la organización cumplir con los requisitos de seguridad de la propia organización estableciendo los 3 principios fundamentales en los que se basa la seguridad informática que son:

- **Confiabilidad de los datos**. Se refiere a la capacidad del sistema para evitar que personas o procesos no autorizados puedan acceder a la información almacenada en él.

- **Disponibilidad de los datos.** Se refiere a él funcionamiento eficientemente y que es capaz de recuperarse rápidamente en caso de falla. Es decir que la información se pueda utilizar cuando se requiera.

- **Integridad de los datos.** El sistema no debe modificar ni corromper la información que almacena, o permitir que alguien no autorizado lo haga. Permitiendo asegurar que no ha sido falsificada la información. Teniendo en cuenta que este tipo de norma puede ser implementada en cualquier tipo de organización ya sea grande, pequeña, privada o pública. Es por este motivo es seleccionada la empresa para la realización de una propuesta de gestión y seguridad basado en la norma ISO 27001:2013

La norma ISO 27001 se convierte en la guía a seguir a través de sus diferentes dominios, lo que permite, implementar, operar, monitorear, revisar y realizar la mejora continua del sistema de gestión de seguridad de información – SGSI, a su

[9] ICONTEC INTERNACIONAL. Sistema de gestión de seguridad de la información. [en línea]. Bogotá: ICONTEC, 2010 [fecha de consulta 5 de octubre de 2017]. Disponible en: http://www.icontec.org/Ser/Ed/Paginas/Sgsi.aspx

vez permite entender e interiorizar en Siselcom S.A.S., el concepto de la seguridad de la información.

En Colombia, el instituto Colombiano de normas técnicas - ICONTEC adopta la norma ISO/IEC 27001:2013 por traducción bajo la referencia ISO/IEC 27001. El establecimiento del SGSI se fundamenta en los documentos y registros requeridos por la revisión 2013 de la norma ISO/IEC 27001 mostrados en el Cuadro 1:

Cuadro 1. Documentación requerida por la norma

Documentos	Capítulo de ISO 27001:2013
El alcance del sistema de gestión de seguridad de la información	4.3
Política de seguridad de la información y objetivos	5.2 y 6.2
Metodología de evaluación y tratamiento de riesgos	6.1.2
Declaración de aplicabilidad	6.1.3 d
Plan de tratamiento de riesgo	6.1.3 e y 6.2
Informe sobre evaluación de riesgos	8.2
Definición de roles y responsabilidades de seguridad	A.7.1.2 y A.13.2.4
Inventario de activos	A.8.1.1
Uso aceptable de los activos	A.8.1.3
Política de control de acceso	A.9.1.1
Procedimientos de operación para gestión de TI	A.12.1.1
Principios de ingeniería de sistemas seguros	A.14.2.5
Política de seguridad para proveedores	A.15.1.1
Procedimiento para gestión de incidentes	A.16.1.5
Procedimientos de Continuidad de negocio	A.17.1.2
Requerimientos legales, regulatorios y contractuales	A.18.1.1

Fuente. 27001ACADEMY. Listado de documentación requerida ISO-27001:2013 [en línea]. Bogotá: Wordpress, 2014 [fecha de consulta 5 de octubre de 2017]. Disponible en: https://lciso27000.files.wordpress.com/2015/02/iso-27001-lista-documentacion-requerida.pdf

De igual forma los registros mostrados en el Cuadro 2 son esenciales, se pueden excluir los controles del Anexo A si una organización determina que no existen riesgos ni otros requisitos que podrían demandar la implementación de un control.

Cuadro 2. Registros mínimos obligatorios por la norma

Registros	Capítulo de ISO 27001:2013
Registros de capacitación, habilidades, experiencia y calificaciones	7,2
Resultados de supervisión y medición	9,1
Programa de auditoría interna	9,2
Resultados de las auditorías internas	9,2
Resultados de la revisión por parte de la dirección	9,3
Resultados de acciones correctivas	10,1
Registros sobre actividades de los usuarios, excepciones y eventos de seguridad	A.12.4.1, A.12.4.3

Fuente. 27001ACADEMY. Listado de documentación requerida ISO-27001:2013 [en línea]. Bogotá: Wordpress, 2014 [fecha de consulta 5 de octubre de 2017]. Disponible en: https://lciso27000.files.wordpress.com/2015/02/iso-27001-lista-documentacion-requerida.pdf

4.1.1.2 ISO/IEC 27002. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. La última edición de 2013 este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de septiembre de 2013.

4.1.1.3 ISO/IEC 27003. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001.

4.1.1.4 ISO/IEC 27004. Son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.

4.1.1.5 ISO/IEC 27005. Trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001.

4.1.1.6 ISO/IEC 27006. Específica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

4.1.1.7 ISO/IEC 27007. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

4.1.1.8 ISO/IEC 27035. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

4.1.2 Sistema de gestión de seguridad de la información. Teniendo en cuenta la norma NTC-ISO-IEC 27001:2013, "gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente"[10].

Un sistema de gestión de seguridad de la información (SGSI), le permite a la organización gestionar de manera efectiva los riesgos asociados a la seguridad sobre sus activos de información mediante la identificación de las amenazas que puedan llegar a comprometer la seguridad de sus activos de información, generando confianza a sus partes interesadas debido a que demuestra que los riesgos de la empresa son debidamente gestionados.

Con el objetivo de garantizar que las organizaciones realizan una correcta gestión de la seguridad de la información, es indispensable contar con un proceso sistemático, documentado y retroalimentado en todo el personal de la empresa. Este proceso, es el que constituye un sistema de gestión de seguridad de la información (SGSI).

4.1.3 Seguridad de la información. La seguridad de la información es "el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma"[11]. La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

[10] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACION ICONTEC. Sistema de gestión de seguridad de la información. [en línea]. Bogotá: ICONTEC, 2013 [fecha de consulta 5 de octubre de 2017]. Disponible en: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf

[11] CORNEJO, M.; GARCÍA, M.; GONZÁLEZ, I.M. y GUERRERO, M.N. Principios de Seguridad Informática en Sistemas de Información. [en línea]. México: Universidad Autónoma del Estado de Hidalgo, 2015 [fecha de consulta 5 de octubre de 2017]. Disponible en: https://www.uaeh.edu.mx /scige/boletin/tlahuelilpan/n6/e5.html

Precisamente la reducción o eliminación de riesgos asociado a una cierta información es el objeto de la seguridad de la información y la seguridad informática. Más concretamente, "la seguridad de la información tiene como objeto los sistemas el acceso, uso, divulgación, interrupción o destrucción no autorizada de información. Los términos seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información"[12].

➢**Confidencialidad.** La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

➢**Integridad.** Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) Grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

➢**Disponibilidad**. La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran[13].

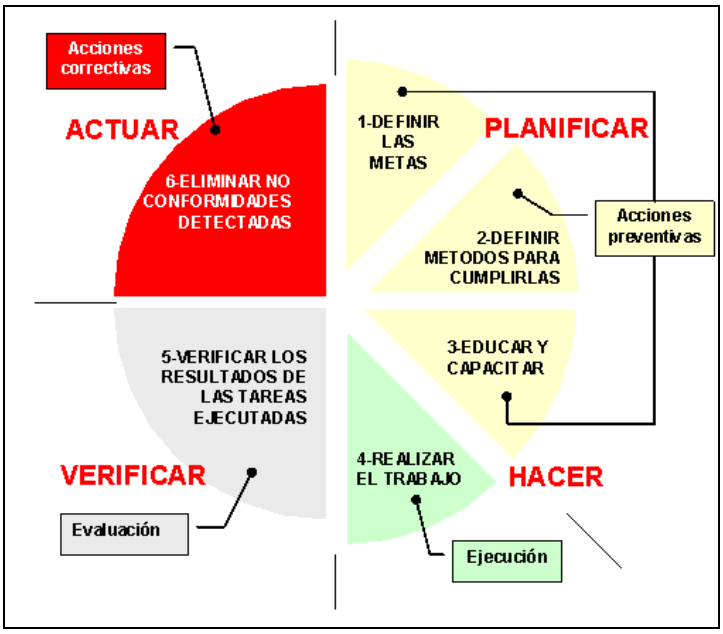
La seguridad de la información dentro de las organizaciones depende del nivel de protección y seguridad de sus activos de información, por lo tanto, es fundamental la implementación de medidas y controles de seguridad adecuados, y el permanente monitoreo, revisión y mejora de los mismos de manera proactiva con el objetivo de garantizar su efectividad.

4.1.4 Ciclo de mejora continua PHVA. El ciclo de mejora continua mostrado en la Figura 2, también conocido como ciclo PDCA (del inglés plan-do-check-act) o PHVA (planificar-hacer-verificar-actuar) o Ciclo de Deming por ser Edwards Deming su creador, es uno de los sistemas más usados para la implementación de un sistema de mejora continua, el cual establece los siguientes cuatro pasos o fases esenciales que de forma sistemática las organizaciones deben llevar a cabo para lograr la mejora continua de sus sistemas de gestión.

[12] HIDALGO LÓPEZ, Celvin Manolo. La firma electrónica avanzada y su certificación. Guatemala: Universidad de San Carlos, 2014. p. 101

[13] ISOTOOLS EXCELLENCE. ISO 27001: ¿Qué significa la Seguridad de la Información?. [en línea]. Bogotá: ISO Tools, 2015 [fecha de consulta 5 de octubre de 2017]. Disponible en: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

Figura 2. Ciclo de mejora continua PHVA



Fuente. WORDPRESS. Ciclo de mejora continua PHVA [en línea]. Bogotá: Blog – Top, 2007 [fecha de consulta 5 de octubre de 2017]. Disponible en: http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

4.1.4.1 Planificar (Plan). En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

- Definir políticas de seguridad.
- Determinar el alcance.
- Valorar activos.
- Analizar el riesgo.
- Aplicar controles de la norma NTC-ISO-IEC 27001:2013.

4.1.4.2 Hacer (Do). En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

- Implementar plan de gestión de riesgos código de práctica para la gestión de la seguridad de la información.

- Implementar controles.

4.1.4.3 Verificar (Check). Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

- Verificación de implementación de gestión de riesgo.
- Revisión de procesos de monitoreo.
- Revisión de niveles de riesgo.
- Revisión de auditorías internas.

4.1.4.4 Actuar (Act). Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

- Implementaciones de mejoras.
- Adoptar medidas preventivas y correctivas.
- Comunicación de resultados.

En nuestro alcance se va tomar la fase de planificación, ya que para la empresa SISELCOM S.A.S., es importante conocer el estado actual de seguridad sobre todos los procesos y estos se logran con el diseño de un sistema de gestión de seguridad de la información.

4.1.5 Definición políticas de seguridad.

- La política de seguridad es "un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma. Las políticas de seguridad definen lo que está permitido y lo que está prohibido, permiten definir los procedimientos y herramientas necesarias, expresan el consenso de los "dueños" y permiten adoptar una buena actitud dentro de la organización"[14].

- Una política de seguridad en el ámbito de la criptografía de clave pública o PKI es "un plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad. Pueden cubrir cualquier cosa desde buenas prácticas para la seguridad de un solo ordenador, reglas de una empresa o edificio, hasta las directrices de seguridad de un país entero"[15].

La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad. Debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos. Debe estar fácilmente accesible de forma que los

[14] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO UNAM. Esquemas de Seguridad Informática. [en Línea]. México: UNAM, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php

[15] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO UNAM. Esquemas de Seguridad Informática. [en Línea]. México: UNAM, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera. Contemplar una política y que haya éxito, corresponde hacer parte a todo el personal de la entidad y de reconocer la información como activo. Por tal razón se deben establecer unos requisitos que se deben establecer para el personal que intervienen directa e indirectamente a los sistemas de información y deben ser de tipo:

- Prohibitiva, es decir, todo lo que no está expresamente permitido está denegado.
- Permisiva, es decir, todo lo que no está expresamente prohibido está permitido.

4.2 MARCO LEGAL

Con el fin de contextualizar el tema de seguridad de la información y la importancia de la misma y considerando el riesgo latente que existe en las entidades privadas y públicas en Colombia, se indica a continuación algunas definiciones y conceptos básicos legales que se deben contemplar para la realización de la propuesta:

- **Ley 1266 del 2008:** por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1581 del 2012:** por la cual se dictan disposiciones generales para la protección de datos personales.

- **Decreto 1377 del 2012:** por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- **Ley 527 de 1999:** por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- **Ley 1273 del 2009:** por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **Decreto 2952 del 2010:** reglamenta los artículos 12 y 13 de la Ley 1266 de 2008, mediante la cual se dictaron disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

5. CONTEXTO ORGANIZACIONAL

5.1 MISIÓN

Contribuir con el desarrollo empresarial de nuestros clientes como proveedor de soluciones integrales de ingeniería en el área de infraestructura eléctrica y de comunicaciones, generado bienestar para nuestros clientes, empleados y accionistas.

5.2 VISIÓN

En el año 2020 ser empresa líder a nivel nacional como integrador de soluciones de ingeniería, siendo reconocidos por la calidad de nuestro servicio, alto grado de innovación, buena disposición del recurso humano y gran aporte social al país.

5.3 RESEÑA HISTÓRICA

SISELCOM S.A.S (SISTEMAS ELÉCTRICOS Y DE COMUNICACIONES SAS) se constituye ante cámara de comercio y DIAN el día 29 de julio de 2013 como sociedad por acciones simplificada por su único socio Fernando Muñoz ingeniero en telecomunicaciones, con sede actual en la ciudad de Bogotá.

SISELCOM S.A.S es una empresa integradora de soluciones de ingeniería en infraestructura eléctrica y de comunicaciones, con representación a nivel nacional, enfocados en satisfacer las necesidades de clientes en el sector industrial, empresarial y comercial. Actualmente cuenta con cuatro (4) empleados directos y un grupo de contratistas especializados en diferentes áreas de ingeniería.

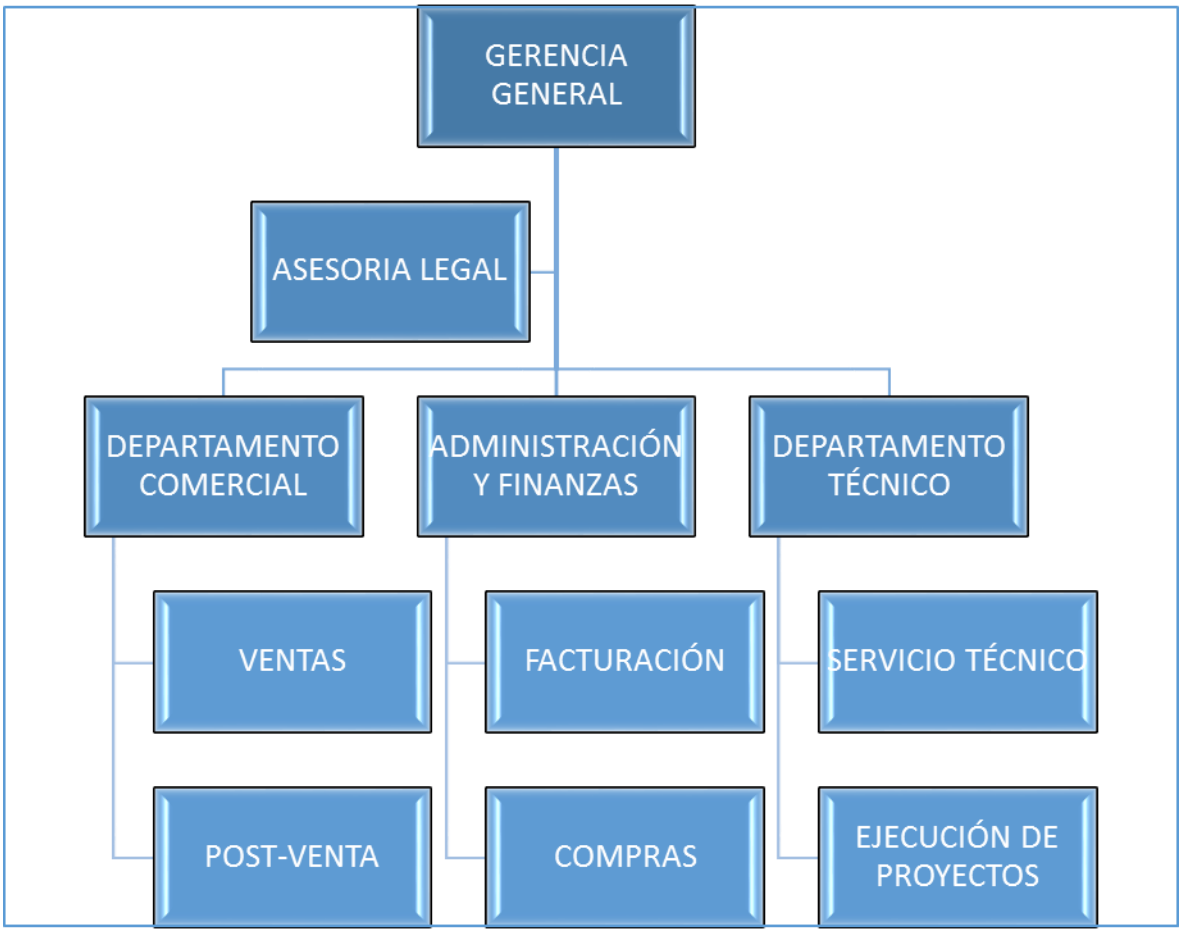
5.4 UBICACIÓN GEOGRÁFICA

SISELCOM S.A.S se encuentra ubicada en la Calle 23F No. 81C- 31 en la ciudad de Bogotá Colombia.

5.5 ESTRUCTURA ORGANIZACIONAL

Como se muestra en la Figura 3, la empresa cuenta en su estructura organizacional con un gerente general, de la cual dependen tres departamentos (departamento comercial, departamento administrativo y financiero, departamento técnico) y un departamento paralelo de asesoría legal.

Figura 3. Organigrama SISELCOM S.A.S



Fuente. Los Autores

Cada uno de los niveles tiene a cargo unas áreas específicas:

➢Fernando Muñoz (gerente general y representante legal): Dirección comercial, financiera, de compras y de ingeniería, supervisión y programación de servicios y ejecución de proyectos.

➢Julián Orjuela (asesor comercial): Elaboración, presentación y seguimiento de ofertas comerciales, consecución de nuevos clientes, proyectos y atención de cuentas existentes, apoyo en programación de servicios.

➢Charly Rocha (asistente contable y administrativo): Manejo y recudo de cartera, manejo de facturación de venta y compra, apoyo en proceso de compras y apoyo en gestión administrativa.

➢Andrea Camargo (contador (personal externo)): Dirección contable, liquidación de impuestos, asesoría financiera.
➢Ana María González (abogado (personal externo)): Dirección jurídica, asesoría jurídica en procesos comerciales y laborales.

➢Servicio técnico: Toda la prestación de servicio técnico se contrata con personal externo, técnicos e ingenieros en diferentes especialidades.

➢Ejecución de proyectos: La ejecución de proyectos se realiza con personal externo, técnicos e ingenieros en diferentes especialidades.

5.6 POLÍTICA INTEGRAL DE LA EMPRESA

SISELCOM S.A.S., Empresa dedicada a la asesoría, construcción y prestación de servicios de ingeniería eléctrica y de comunicaciones en el área de suministros, mantenimientos y alquiler de UPS, redes eléctricas, cableado estructurado, acondicionamiento ambiental y circuito cerrado de televisión, da a conocer a continuación su política integral, basada en la Seguridad y Salud de sus Colaboradores y la calidad de sus servicios, comprometiéndose así con:

Satisfacer las necesidades y expectativas de sus clientes, manteniendo la permanencia, competitividad, rentabilidad y liderazgo en el mercado.

➢Mejorar continuamente la eficiencia y eficacia del Sistema de Gestión Integral a través del buen desarrollo de sus procesos, para ofrecer servicios de alta calidad por medio de la generación de soluciones óptimas y factibles para sus clientes.

➢Identificar los peligros, evaluar, valorar, minimizar y controlar los riesgos laborales, con el fin de prevenir la ocurrencia de accidentes y enfermedades laborales para proteger la Seguridad y Salud física, mental y social de sus trabajadores, contratistas y subcontratistas.

➢Prevenir la ocurrencia de accidentes de tránsito por medio de la implementación de programas de seguridad vial con alcance para trabajadores, contratistas y subcontratistas.

➢Cumplir con los requisitos legales nacionales, locales, reglamentarios, de seguridad y salud en el trabajo y otros requisitos que la empresa defina.

➢Fortalecer el potencial humano y profesional de sus colaboradores y lograr un equipo sólido, competente y comprometido que desarrolle el trabajo de forma ética, eficiente y segura.

➢Proveer oportunamente los recursos humanos, físicos y financieros para el mantenimiento y mejoramiento continuo del Sistema de Gestión Integral.

Se mantendrá la difusión de esta Política a toda la empresa y partes interesadas, con el fin de comprometer a los involucrados en el mejoramiento continuo del Sistema de Gestión Integral.

5.7 POLÍTICA DE PREVENCIÓN DE LA FARMACODEPENDENCIA, ALCOHOL Y TABAQUISMO

SISELCOM S.A.S., Empresa dedicada a la asesoría, construcción y prestación de servicios de ingeniería eléctrica y de comunicaciones en el área de suministros, mantenimientos y alquiler de UPS, redes eléctricas, cableado estructurado, acondicionamiento ambiental y circuito cerrado de televisión, considera que en el lugar de trabajo se debe garantizar la seguridad, la salud y el bienestar de toda la empresa, por lo que adquiere el compromiso de generar un ambiente de trabajo sano, seguro y adecuado para sus colaboradores, clientes y demás partes interesadas, a través de las siguientes acciones:

- Desarrollar y mantener actividades de promoción y prevención en seguridad y salud en el trabajo.

- Mantener las instalaciones libres de humo de tabaco.

- Prohibir el consumo de alcohol, tabaco y fármaco dependientes en horario laboral o en cualquier otra actividad en representación de la empresa.

- Monitorear y vigilar periódicamente el uso de estas sustancias por parte de trabajadores, contratistas y/o subcontratistas.

- Tomar medidas disciplinarias en caso de confirmación de sospechas de colaboradores bajo efectos de estas sustancias.

Se mantendrá la difusión de esta Política a toda la empresa y partes interesadas, con el fin de comprometer a los involucrados en el cumplimiento del presente documento.

5.8 REGLAMENTO DE HIGIENE Y SEGURIDAD INDUSTRIAL

5.8.1 Actividad económica. Empresas dedicadas a trabajos de electricidad, incluye solamente empresas dedicadas a las instalaciones eléctricas, en casa de habitación y/o edificios.

5.8.2 Código de actividad económica. Definido con el código 4542 según Decreto 1607 DE 2002. Prescribe el siguiente reglamento, contenido en los siguientes términos:

✓Artículo 1: La empresa se compromete a dar cumplimiento a las disposiciones legales vigente, tendientes a garantizar los mecanismos que aseguren una adecuada y oportuna prevención de los accidentes de trabajo y enfermedades profesionales, de conformidad con los Artículos 34, 57, 58, 108, 205, 206, 217, 220, 221, 282, 283, 348, 349, 350 y 351 del Código Sustantivo del Trabajo, la Ley 9ª de 1979, resolución 2400 de 1979, Decreto 614 de 1984, Resolución 2013 de 1986, Resolución 1016 de 1989, Resolución 6398 de 1991, Decreto 1295 de 1994, Decreto 1772 de 1994, Decreto 1443 de 2014, Decreto 1072 de 2015 y demás normas que con tal fin se establezcan.

✓Artículo 2: La empresa se obliga a promover y garantizar la constitución y funcionamiento del Vigía en SST, de conformidad con lo establecido por el Decreto 614 de 1984, Resolución 2013 de 1986, Resolución 1016 de 1989, Decreto 1295 de 1994, Decreto 1072 de 2015.

✓Artículo 3: La empresa se compromete a designar los recursos necesarios para desarrollar actividades permanentes, de conformidad con el SG-SST, elaborado de acuerdo al Decreto 614 de 1984 y Resolución 1016 de 1989, el cual contempla como mínimo, los siguientes aspectos:

➢Promover y mantener el más alto grado de bienestar físico, mental y social de los trabajadores, en todos los oficios; prevenir cualquier daño a la salud, ocasionado por las condiciones de trabajo; protegerlos en su empleo de los riesgos generadores por la presencia de agentes y procedimientos nocivos; Colocar y mantener al trabajador en una actividad acorde con sus aptitudes fisiológicas y psicosociales.

➢Establecer las mejores condiciones de Saneamiento Básico Industrial y crear los procedimientos que conllevan a eliminar o controlar los factores de riesgo que se originen en los lugares de trabajo y que puedan ser causa de enfermedades o accidentes.

✓Artículo 4: Los riesgos existentes en la empresa mostrados en el Cuadro 3, están constituidos principalmente por:

Cuadro 3. Clasificación de peligros

Identificación	Clasificación
Biológicos	Virus, hongos, bacterias
Biomecánicos	Movimientos repetitivos
Biomecánicos	Posturas mantenidas
Biomecánicos	Manipulación de cargas
Biomecánicos	Postura prolongada
Biomecánicos	Esfuerzo
Biomecánicos	Levantamiento de cargas

Cuadro 3. (Continuación)

Identificación	Clasificación
Condiciones de Seguridad	Mecánico
Condiciones de Seguridad	Público
Condiciones de Seguridad	Eléctrico
Condiciones de Seguridad	Accidente de Transito
Condiciones de Seguridad	Locativo
Condiciones de Seguridad	Tecnológico
Condiciones de Seguridad	Trabajo en altura
Fenómenos Naturales	Terremoto, inundación
Físico	Ruido
Físico	Vibración
Físico	Iluminación
Físico	Radiaciones no ionizantes
Psicosocial	Condiciones de la tarea
Psicosocial	Condiciones del trabajo
Psicosocial	Gestión organizacional
Psicosocial	interface personal tarea
Químico	Material particular
Químico	Contacto con sustancias químicas
Químico	Vapores
Químico	Inhalación de gases, polvos, vapores, humos metálicos
Químico	Líquidos, gases, vapores

Fuente. Los Autores

✓Parágrafo: a efecto de que los riesgos contemplados en el presente Artículo, no se traduzcan en accidente de trabajo o enfermedad profesional, la empresa ejerce su control en la fuente, en el medio transmisor o en el trabajador, de conformidad con lo estipulado en el Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) de la empresa, el cual se dé a conocer a todos los trabajadores al servicio de ella.

✓Articulo 5: la empresa y sus trabajadores darán estricto cumplimiento a las disposiciones legales, así como las normas técnicas e internas que se adopten para lograr la implementación de las actividades de Medicina Preventiva y del Trabajo, Higiene y Seguridad Industrial, que sean concordantes con el presente Reglamento y con el SG-SST de la empresa.

✓Artículo 6: la empresa ha implantado un proceso de inducción del trabajador a las actividades que debe desempeñar, capacitándolo respecto a las medidas de prevención y seguridad que exija el medio ambiente laboral y el trabajo específico que vaya a realizar.

✓Artículo 7: este reglamento permanecerá exhibido en, por lo menos dos lugares visibles de los locales de trabajo, junto con la resolución aprobatoria, cuyos contenidos se dan a conocer a todos los trabajadores en el momento de su ingreso.

✓Articulo 8: el presente reglamento entra en vigencia a partir de la aprobación impartida por el Ministerio de Protección Social y durante el tiempo que la empresa conserve, sin cambios sustanciales, las condiciones existentes en el momento de su aprobación, tales como la Actividad Económica, métodos de producción, instalaciones locativas o cuando se dicten disposiciones gubernamentales que modifiquen las normas del Reglamento o que limiten su vigencia.

5.9 PROCESOS QUE MANEJA LA EMPRESA

➢**Proceso administrativo y financiero.** En dirección de Fernando Muñoz, con asesoría de Andrea Camargo (Contador) en el área financiera y contable, asesoría de Ana María González en el área jurídica y apoyo de Charly Rocha en diferentes funciones.

➢**Proceso de compras.** En dirección de Fernando Muñoz, con apoyo de Charly Rocha en gestión de órdenes de compra y facturación de compra.

➢**Proceso comercial.** Proceso en dirección de Fernando Muñoz, Julián Orjuela como ejecutivo comercial y Johana Matiz como gestor de mercadeo.

➢**Proceso de contratación.** En dirección de Fernando Muñoz, con la asesoría legal realiza entrevista y proceso de contratación del personal fijo y externo.

➢**Proceso ingeniería y área técnica.** Proceso en dirección de Fernando Muñoz, Apoyo en coordinación de servicios por Julián Orjuela, ejecución de servicios por personal contratistas relacionados en el Cuadro 4.

Cuadro 4. Distribución de responsabilidades

Nombre	Área Técnica
Cesar Bonilla	Redes eléctricas y plantas eléctricas
Aristi Jiménez	Redes eléctricas y plantas eléctricas
Christian Camargo	Seguridad electrónica
Diego Vargas	UPS
Edgar Sierra	UPS
Edwin Esteban González	UPS
Fernando Martínez	UPS
Francisco Montañez	UPS
Jhon Guerra	UPS Valle del Cauca
Jonatán Cuervo	UPS

Cuadro 4. (Continuación)

Nombre	Área Técnica
Mauricio Riaño	UPS
Wilber Iturre	Ingeniería
Wilson Ernesto Chaparro	UPS
Hosni Benavidez	Redes de datos
Edwin Estévez Blanco	UPS
Néstor Ríos	Aires Acondicionados
Jaime Alonso	Aires Acondicionados
Andrés Guaraca	Aires Acondicionados
Jhon Betancourt	Aires Acondicionados
Hugo Carrillo	Transportes
Rafael Arias Fonseca	Transportes

Fuente. Los Autores

6. METODOLOGÍA

6.1 DISEÑO

En el proceso de levantamiento de la información se realiza desde el concepto académico, que permite evidenciar los riesgos que amenazan la seguridad de la información dentro de la empresa SISELCOM por medio de entrevistas con todo el personal que participa de los procesos en la empresa (personal de planta). Los procesos realizados en el levantamiento información se describen a continuación.

- Entrevistas con la gerencia.
- Visitas de campo.
- Verificación de inventario.
- Valoración de activos de acuerdo al Anexo B de la norma ISO 27005.
- Validación de controles de acuerdo al Anexo A de la norma ISO 27001:2013.
- Análisis de riesgo basado en la norma ISO 27001:2013.

6.2 PARTICIPANTES

La gerencia como cabeza de la empresa y todos los trabajadores que participan en los procesos, manipulan o acceden a los sistemas de información de la empresa ya sea como personal contratista, externo o directo. En el proceso de levantamiento de información intervinieron las siguientes áreas:

- Área Comercial.
- Área jurídica.
- Área administrativa.
- Área de contaduría.

6.3 INSTRUMENTOS

Se realizó una entrevista a cada persona vinculada a la empresa con preguntas diseñadas de acuerdo con su rol dentro de la empresa. Adicionalmente se verifico toda la documentación existente, se validaron todos los procesos y su funcionamiento para luego realizar la valoración de activos y el análisis de riesgo.

7. ESTADO ACTUAL DE LA SEGURIDAD

Para la organización el propósito de conocer, la importancia de la seguridad de la información para el personal; se aplicó una encuesta la cual permitió conocer la percepción de los empleados en cuanto a la seguridad, la encuesta consistió en 39 preguntas algunas de respuesta abierta con las cuales se establece el estado actual de seguridad dentro de la empresa.

Se aplicó a las cuatro (4) personas que actualmente se encuentran vinculadas directamente con la empresa y son las que conocen todo el manejo de datos dentro de la organización y acceso a la red. Con la ayuda de la herramienta WEB online encuesta, se realizó la toma y digitalización en el siguiente link: https://www.onlineencuesta.com/s/f612391.

7.1 RESULTADOS ENCUESTA REALIZADA A USUARIOS

En la encuesta realizada se procedió a realizar un análisis de los resultados obtenidos, ya que las preguntas son de tipo cerrado y abierto, las respuestas abiertas van concatenadas con una pregunta cerrada así que se analizaran en conjunto donde se aplique.

7.1.1 Resultado pregunta No. 1. Para conocer el rol de los participantes dentro de la organización se consultó por su cargo dentro de la empresa se obtuvieron los resultados relacionados en el Cuadro 5.

Cuadro 5. Resultados pregunta No. 1

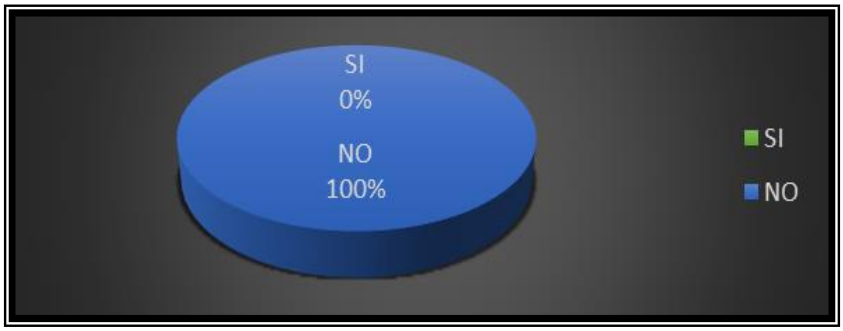
1. ¿Cuál es su rol dentro de la empresa?	
1.	Comercial
2.	Asesor jurídico
3.	Asistente administrativo y contable
4.	Contadora publica

Fuente. Los Autores

El proceso de encuestas se realiza a las personas que participan en el día a día de la operación de la empresa, en el manejo de las herramientas y conocen el tratamiento de datos.

7.1.2 Resultado pregunta No. 2

Figura 4. ¿Sabe si la empresa cuenta con una política de seguridad informática?

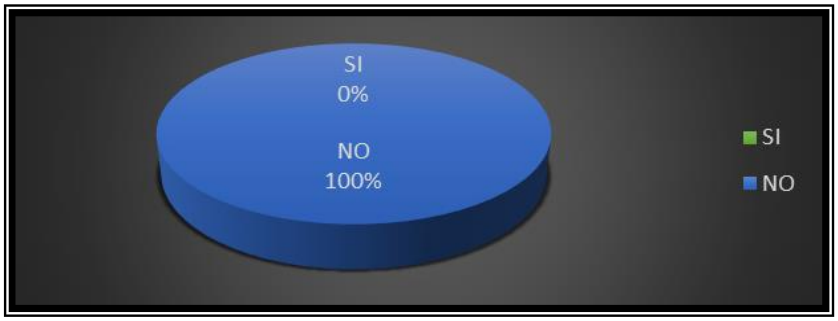


Fuente. Los Autores

De acuerdo con las respuestas de la pregunta 2 mostradas en la Figura 4, donde el 100% de los encuestados indica que no existen políticas de seguridad de la información se evidencia un incumplimiento del numeral A.5 (Políticas de la seguridad de la información) del anexo A de la norma ISO 27001:2013.

7.1.3 Resultado pregunta No. 3. De ser afirmativa por favor explique brevemente lo que conoce de la política, como la respuesta fue negativa en todos los casos como se muestra en la Figura 5, no aplica esta pregunta.

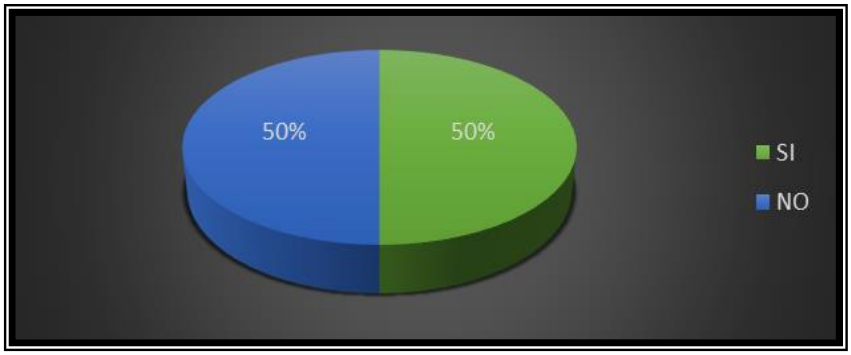
Figura 5. ¿De ser afirmativa la pregunta No. 2 por favor explique brevemente lo que conoce de la política?



Fuente. Los Autores

7.1.4 Resultado pregunta No. 4.

Figura 6. ¿Al manejar un proyecto sabe si se tiene en cuenta la seguridad de la información?



Fuente. Los Autores

7.1.5 Resultado pregunta No. 5

Cuadro 6. ¿De qué manera se toma en cuenta?

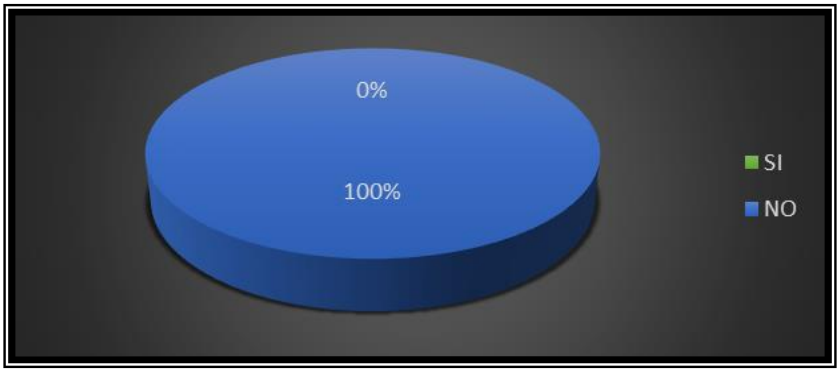
Encuesta	Respuesta
1.	Almacenamiento de la información, ubicación, medios de almacenamiento, etc.
2.	Se hace acuerdo de confidencialidad a los trabajadores, en los contratos de prestación de servicios de pacta también una cláusula de confidencialidad que protege tanto al contratista como al contratante.

Fuente. Los Autores

En las respuestas de las preguntas 4 y 5 se evidencia que no se tiene claro el manejo de la seguridad de la información en la gestión de proyectos, ya que solo el 50% de los encuestados contesto afirmativamente como lo muestra la Figura 6, en la pregunta 5 las dos personas contestaron de manera adecuada como lo muestra el Cuadro 6, lo que muestra un incumplimiento del numeral A.6.1 (Organización de la seguridad de la información) en especial el numeral A.6.1.5 (Seguridad de la información en la gestión de proyectos) del anexo A de la norma ISO 27001:2013.

7.1.6 Resultado pregunta No. 6

Figura 7. ¿Conoce si la empresa tiene una política acerca del uso de dispositivos móviles o de teletrabajo?

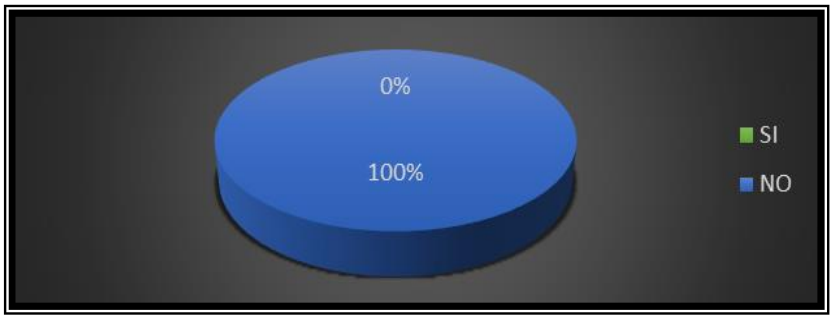


Fuente. Los Autores

De acuerdo con las respuestas de la pregunta 6 mostradas en la Figura 7, donde el 100% de los encuestados contesto negativamente acerca de las políticas del uso de dispositivos móviles o teletrabajo se observa un incumplimiento del numeral A.6.2 (Dispositivos móviles y teletrabajo) del anexo A de la norma ISO 27001:2013.

7.1.7 Resultado pregunta No. 7. De existir por favor explique cómo funciona esta política. Como se muestra en la Figura 8, se obtuvo respuesta negativa en la pregunta anterior esta no aplica.

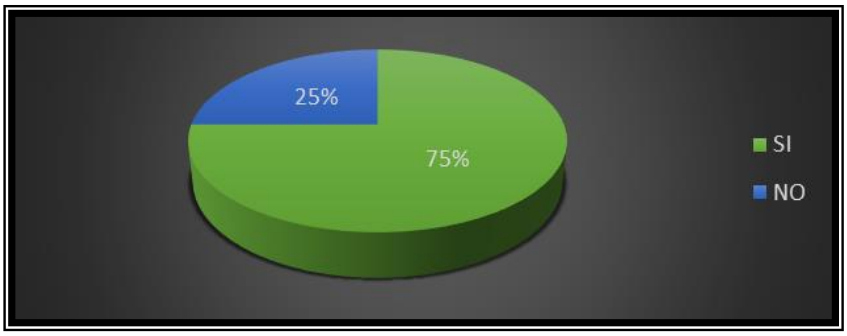
Figura 8. De existir la política de uso de dispositivos móviles por favor explique cómo funciona esta política.



Fuente. Los Autores

7.1.8 Resultado pregunta No. 8

Figura 9. ¿Sabe si en su contrato existe un acuerdo de confidencialidad y sus responsabilidades con la empresa?



Fuente. Los Autores

7.1.9 Resultado pregunta No. 9. En los casos donde se obtuvieron respuestas afirmativas en la pregunta anterior se obtuvieron las siguientes respuestas:

Cuadro 7. De existir por favor describir lo que conoce de este acuerdo

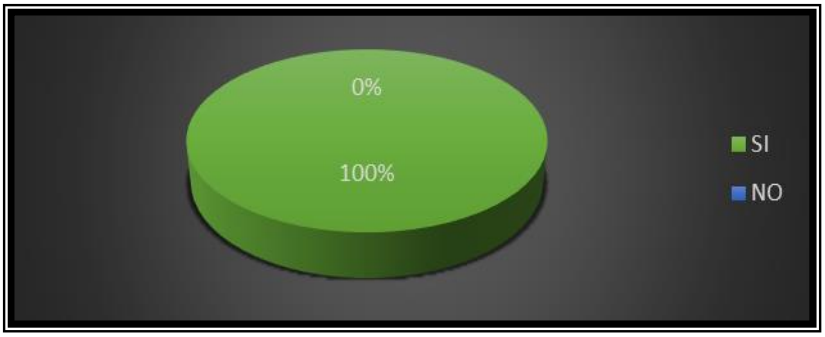
Encuesta	Respuesta
1.	No divulgar información confidencial, precios, proveedores, información financiera y en general toda aquella que no esté autorizada.
2.	Actualmente no mantenemos un contrato solo presto asesoría jurídica cuando se crea necesario facturo sobre servicio y por lo tanto también tengo claro que la información que yo tenga conocimiento en el tiempo que realice mis servicios se le debe dar un trato confidencial
3.	Conoce y acepta las normas legales de Siselcom, conciencia de las consecuencias del incumplimiento, no se puede circular información de bases de datos, ni de clientes ni proveedores.

Fuente. Los Autores

De acuerdo con el resultado en las preguntas 8 y 9, mostrados en la Figura 9 y Cuadro 7 respectivamente, donde el 75% de los encuestados contesto afirmativamente en cuanto a acuerdos de confidencialidad y responsabilidades, se observa un incumplimiento el numeral A.7.1.2 (Términos y condiciones del empleo) y A.13.2.4 (Acuerdos de confidencialidad o de no divulgación) del anexo A de la norma ISO 270001:2013 pero se observa un poco de desinformación en lo que incluyen estos acuerdos.

7.1.10 Resultado pregunta No. 10

Figura 10. ¿Conoce quien administra el inventario de activos de la empresa?



Fuente. Los Autores

7.1.11 Resultado pregunta No. 11

Cuadro 8. Indique quien es la persona encargada

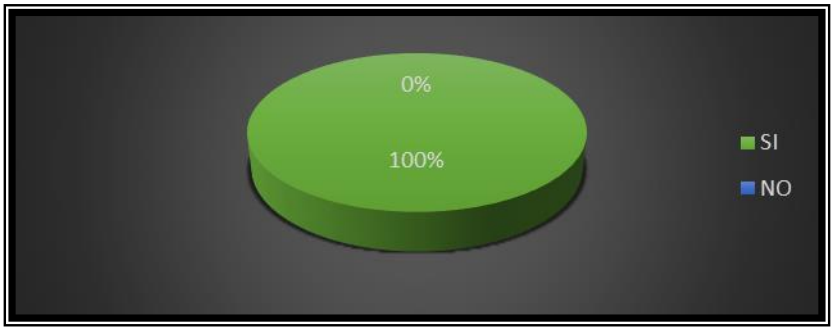
Encuesta	Respuesta
1.	Ingeniero de proyectos
2.	Charly ella es la auxiliar administrativa y contable de la empresa
3.	Fernando Muñoz
4.	Fernando Muñoz

Fuente. Los Autores

En los resultados de las preguntas 10 y 11 se observa un incumplimiento del numeral A.8.1.1 (Inventario de activos) del anexo A de la norma ISO 27001:2013 ya que como lo muestra la Figura 10 el 100% de los encuestados, contesto que conoce quien administra el inventario de activos, pero al preguntar qué persona es la encargada en el Cuadro 8 no se tiene claridad en el personal, esta desinformación puede causar mal manejo del inventario y de los activos.

7.1.12 Resultado pregunta No. 12

Figura 11. ¿Sabe que activos de la empresa están bajo su responsabilidad?



Fuente. Los Autores

De acuerdo con las respuestas de la pregunta 12 como lo muestra la Figura 11 el 100% de los encuestados contesto negativamente acerca de si saben que activos estaban bajo su responsabilidad.

7.1.13 Resultado pregunta No. 13

Cuadro 9. Indique los activos

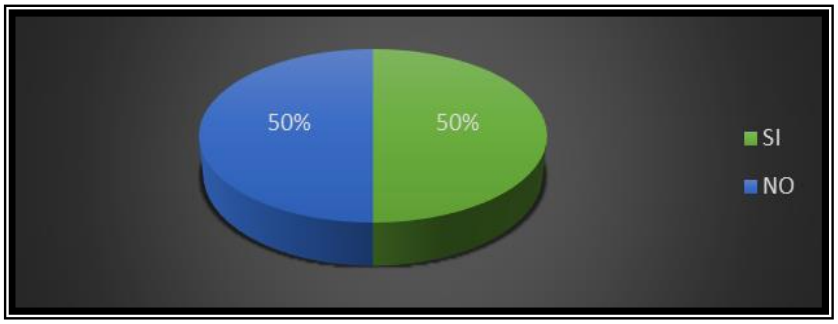
Encuesta	Respuesta
1.	Celular, computador portátil, escritorios, sillas, implementos de oficina.
2.	información contratos proveedores y clientes
3.	Computador y accesorios, escritorio de oficina
4.	Computador

Fuente. Los Autores

En los resultados de las preguntas 12 y 13 donde el 100% de los encuestados respondió que conoce que activos de la empresa están bajo su responsabilidad y con la respectiva identificación de estos en el Cuadro 9, podemos evidenciar un cumplimiento del numeral A.8.1.2 (Propiedad de los activos) del anexo A de la norma ISO 27001:2013.

7.1.14 Resultado pregunta No. 14

Figura 12. ¿Maneja dispositivos extraíbles como memorias USB, CD, DVD entre otros?

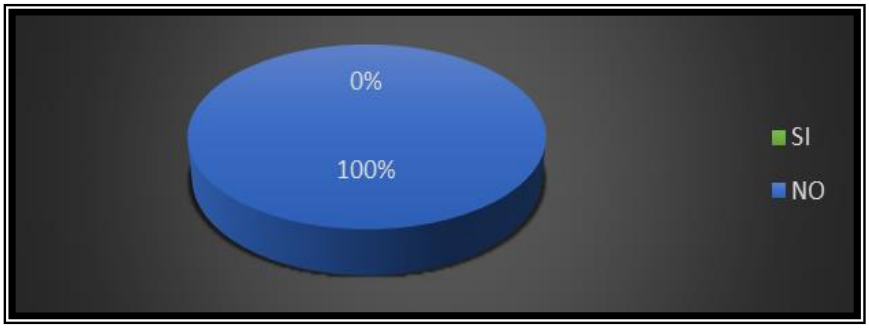


Fuente. Los Autores

Como lo muestra la Figura 12 el 50% de los encuestados maneja dispositivos extraíbles.

7.1.15 Resultado pregunta No. 15

Figura 13. ¿Sabe si la empresa cuenta con algún tipo de restricción acerca del uso de estos dispositivos?

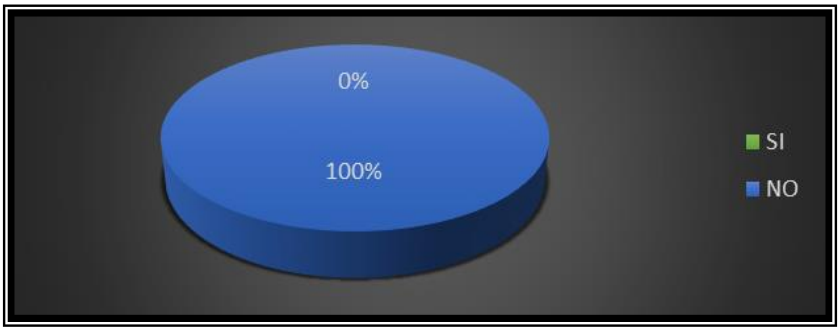


Fuente. Los Autores

De acuerdo con las respuestas de la pregunta 15 mostradas en la Figura 13 el 100% de los encuestados contesto negativamente acerca de si la empresa cuenta con algún tipo de restricción acerca del uso de estos dispositivos.

7.1.16 Resultado pregunta No. 16. De ser afirmativa indique cual es la restricción, como se obtuvo respuesta negativa en la pregunta anterior esta no aplica como lo muestra la Figura 14.

Figura 14. De ser afirmativa indique cual es la restricción acerca del uso de dispositivos

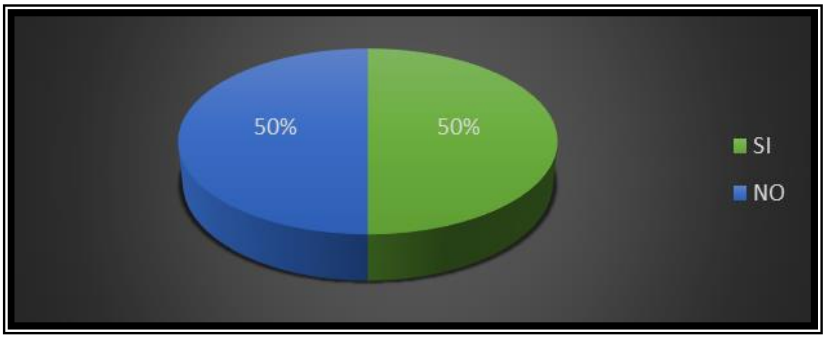


Fuente. Los Autores

Teniendo en cuenta los resultados de las preguntas 14, 15 y 16 donde el 50% de los encuestados indica que usa dispositivos removibles y el 100% indica que no existen restricciones acerca del uso de estos dispositivos podemos observar un incumplimiento del numeral A.8.3 (Manejo de medios) del anexo A de la norma ISO 27001:2013.

7.1.17 Resultado pregunta No. 17

Figura 15. ¿Para el ingreso a los equipos propiedad de la empresa maneja algún tipo de usuario o clave?

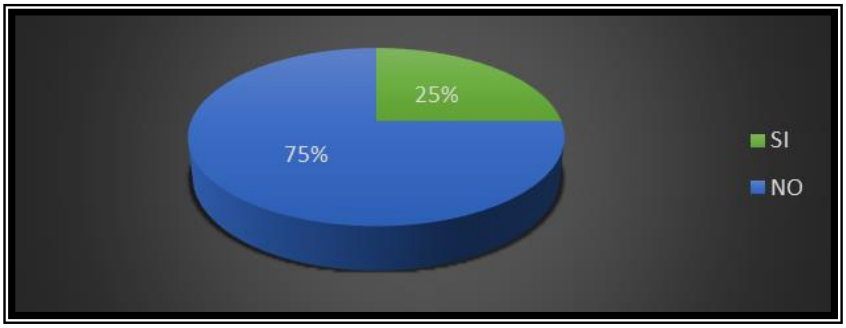


Fuente. Los Autores

De acuerdo con el resultado de la pregunta 17 mostrado en la Figura 15, el 50% de los encuestados indica que no maneja ningún tipo de usuario o clave, podemos evidenciar un incumplimiento del numeral A.9 (Control de acceso) del anexo A de la norma ISO 27001:2013.

7.1.18 Resultado pregunta No. 18

Figura 16. ¿Considera que las contraseñas que usted utiliza para acceder a la información de la empresa son de alta seguridad?



Fuente. Los Autores

Como lo muestra la Figura 16 solo el 25% de los encuestados considera que las contraseñas son de alta seguridad.

7.1.19 Resultado pregunta No. 19

Cuadro 10. Tipo de contraseñas que utiliza

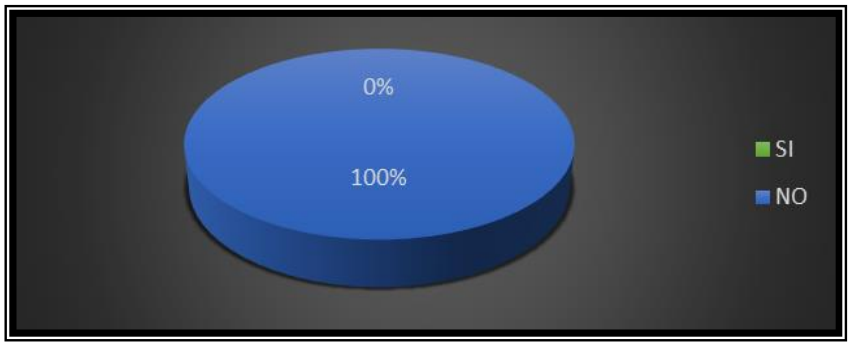
Encuesta	Respuesta
1.	Combinación de mayúsculas y minúsculas, signos de puntuación y números.
2.	Nombre de mascota y números.
3.	Por ejemplo, el nombre de la empresa y un número o en otros casos la sigla junto o NIT
4.	Caracteres y números.

Fuente. Los Autores

Los resultados de las preguntas 18 y 19 donde el 75% de los encuestados indica que las contraseñas que maneja son de alta seguridad al preguntar qué tipo de contraseñas utiliza en el Cuadro 10 se puede ver que no son seguras por lo que se observa un incumplimiento del numeral A.9.4.3 (Sistema de gestión de contraseñas) del anexo A de la norma ISO 27001:2013.

7.1.20 Resultado pregunta No. 20

Figura 17. ¿Conoce el plan de contingencia de la empresa en caso de desastre natural?

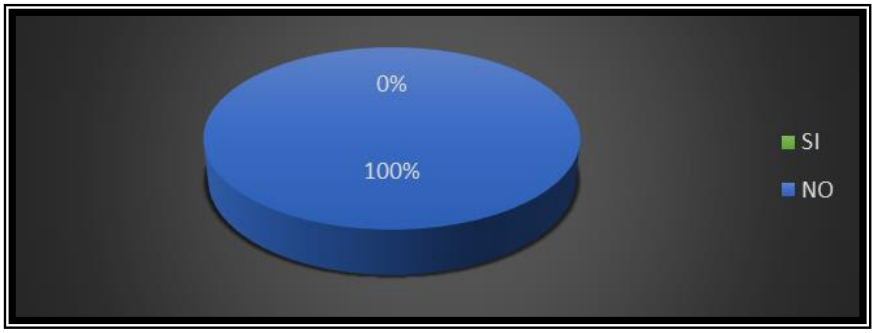


Fuente. Los Autores

De acuerdo con las respuestas de la pregunta 20 mostradas en la Figura 17, el 100% de los encuestados contesto negativamente acerca de si conoce el plan de contingencia de la empresa en caso de desastre natural.

7.1.21 Resultado pregunta No. 21. De conocerlo indique como funciona este plan, como se obtuvo respuesta negativa en la pregunta anterior esta no aplica como lo muestra la Figura 18.

Figura 18. De conocerlo indique cómo funciona el plan de contingencia

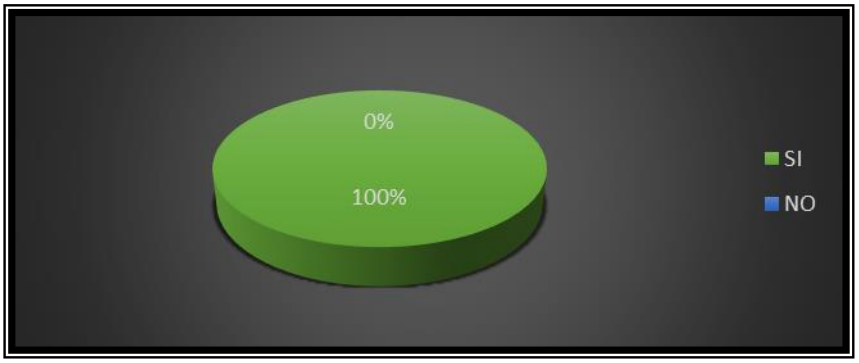


Fuente. Los Autores

Las respuestas de las preguntas 20 y 21 donde el 100% de los encuestados indica que no conoce o no existe un plan de contingencia en caso de desastre vemos un incumplimiento de los numerales A.11 (Seguridad física y del entorno) y A.17 (Aspectos de seguridad de la información de la gestión de continuidad de negocio) del anexo A de la norma ISO 27001:2013.

7.1.22 Resultado pregunta No. 22

Figura 19. ¿Cree usted que maneja información crítica o sensible de la empresa?



Fuente. Los Autores

De acuerdo con los resultados mostrados en la Figura 19, el 100% de los encuestados considera que maneja información sensible.

7.1.23 Resultado pregunta No. 23

Cuadro 11. De ser afirmativa por favor indique que tipo de información maneja

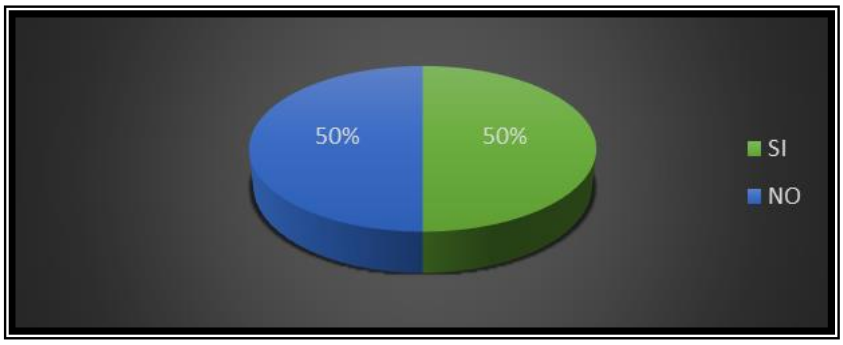
Encuesta	Respuesta
1.	Proveedores, listados de precios, información comercial, información financiera, información del cliente, entre otros.
2.	Información de carácter confidencial y de uso restringido
3.	datos bancarios, contraseñas
4.	Financiera

Fuente. Los Autores

Los resultados de las preguntas 22 y 23 se puede observar que el 100% de los encuestados poseen información sensible de la empresa, en el Cuadro 11 se evidencia el tipo de información que manejan los encuestados; esto permite indicar que el numeral A.7 (Seguridad de los Recursos Humanos) del anexo A de la norma ISO 27001:2013 se está cumpliendo.

7.1.24 Resultado pregunta No. 24

Figura 20. ¿Cree que en el manejo de esta información existe un riesgo probable de pérdida o daño?



Fuente. Los Autores

Como lo muestra la Figura 20 el 50% de los encuestados cree que es probable que la información critica se pueda perder o dañar.

7.1.25 Resultado pregunta No. 25

Cuadro 12. Ejemplo de riesgo

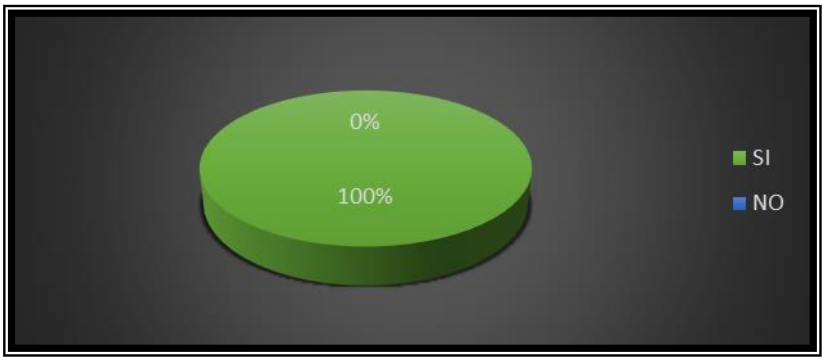
Encuesta	Respuesta
1.	Robo de computador y/o celular.
2.	Que el computador presente daños

Fuente. Los Autores

Los resultados de las preguntas 24 y 25 se puede observar que el 50% de los encuestados desconocen los riesgos que existen en la compañía frente a la información que se maneja y como lo muestra el Cuadro 12 los encuestados indican que los unicos riesgos que existen son el robo o daño del computador, esto permite indicar que el numeral A.11 (Seguridad física y del entorno) de la norma ISO 27001:2013 se está incumpliendo.

7.1.26 Resultado pregunta No. 26

Figura 21. ¿Conoce las implicaciones que conllevan una posible pérdida o daño de información?



Fuente. Los Autores

7.1.27 Resultado pregunta No. 27

Cuadro 13. Cuáles serían las posibles implicaciones

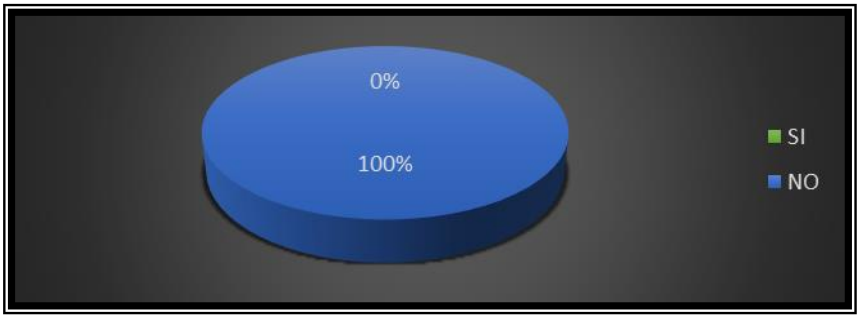
Encuesta	Respuesta
1.	Trazabilidad de la información, archivo, información de clientes, contactos con proveedores, etc.
2.	puede significar un riesgo financiero a la empresa y más si esta información es utilizada por terceros
3.	La empresa se vería expuesta a revelar información confidencial, mayores costos para la empresa, pérdida de tiempo al momento de recuperar la información,
4.	Reprocesos, sanciones

Fuente. Los Autores

Las respuestas de las preguntas 26 y 27 se puede observar en la Figura 21 que el 100% de los encuestados indica que conoce las implicaciones de una posible pérdida o daño de información pero al preguntar cuáles son las posibles implicaciones en el Cuadro 13 vemos desinformación de estas implicaciones lo que nos muestra un incumplimiento de los numerales A.7.2 (Durante la ejecución del empleo), A.17 (Aspectos de seguridad de la información de la gestión de continuidad de negocio) y A.18 (Cumplimiento) del anexo A de la norma ISO 27001:2013.

7.1.28 Resultado pregunta No. 28

Figura 22. ¿Los activos de la empresa son debidamente protegidos cuando no están en las instalaciones de la organización?



Fuente. Los Autores

7.1.29 Resultado pregunta No. 29

Cuadro 14. Razón por la cual los activos de la empresa son debidamente protegidos

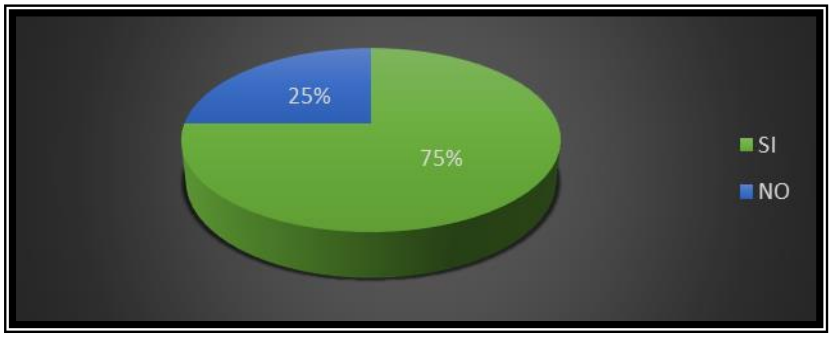
Encuesta	Respuesta
1.	No existe un seguro contra robo, perdida o daño.
2.	No lleva una relación en Excel de cuales activos se encuentran por fuera, sin embargo, la información está protegida por cláusulas de confidencialidad
3.	Son fijos en las instalaciones y cualquiera puede hacer uso de este.
4.	No se lleva un control.

Fuente. Los Autores

Los resultados obtenidos en las preguntas 28 y 29 en la Figura 22 donde el 100% de los encuestados indica que los activos no están debidamente protegidos cuando se encuentran fuera de la organización y en el Cuadro 14 se listan las razones dadas por los encuestados observamos un incumplimiento de los numerales A.8 (Gestión de activos) y A.11 (Seguridad física y del entorno) del anexo A de la norma ISO 27001:2013.

7.1.30 Resultado pregunta No. 30

Figura 23. ¿Sabe si el equipo que maneja tiene instalado algún tipo de antivirus o protección?

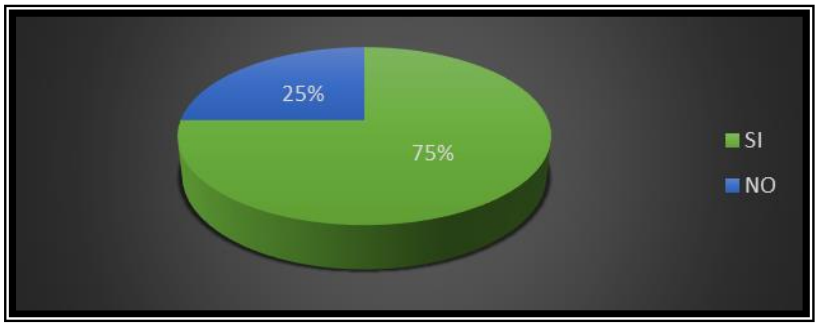


Fuente. Los Autores

En los resultados de la pregunta 30 en la Figura 23 se puede observar que el 75% de los encuestados poseen en sus ordenadores antivirus; se identifica que se cumplen con algunos de los controles, pero no satisfactoriamente, por lo tanto, se deben generar cambios para el cumplimiento del numeral A.12 (Seguridad en las operaciones) del Anexo A norma ISO 27001:2013).

7.1.31 Resultado pregunta No. 31

Figura 24. ¿Realiza copias de seguridad de la información que maneja o sabe si la empresa realiza este proceso?

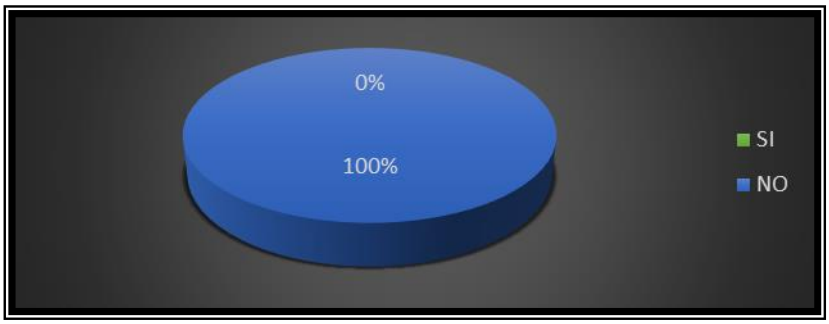


Fuente. Los Autores

En la Figura 24 se muestran las respuestas de la pregunta 31 donde el 75% de los encuestados indica que se realizan copias de seguridad de la información se evidencia un cumplimiento del numeral A.12.3 (Copias de respaldo) del anexo A de la norma ISO 27001:2013.

7.1.32 Resultado pregunta No. 32

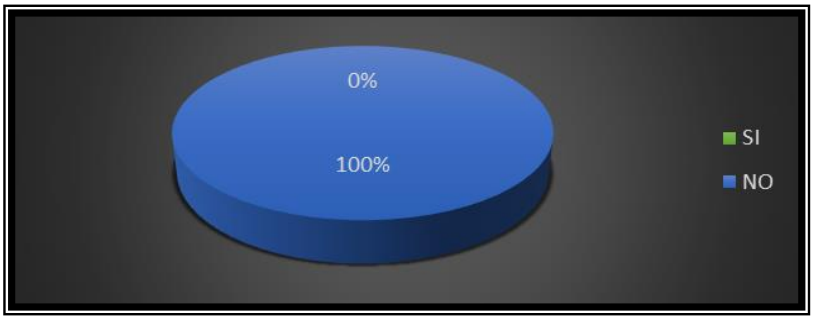
Figura 25. ¿Sabe si se realiza mantenimiento a los equipos de la empresa regularmente?



Fuente. Los Autores

7.1.33 Resultado pregunta No. 33. Indique con qué frecuencia, como se obtuvo respuesta negativa en la pregunta anterior esta no aplica.

Figura 26. Indique con qué frecuencia se realiza este mantenimiento

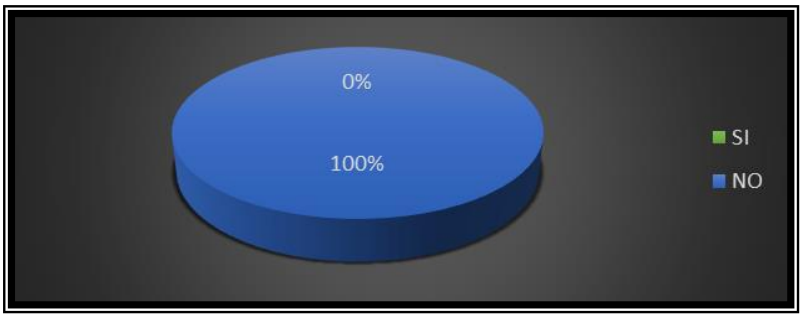


Fuente. Los Autores

Con los resultados de la pregunta 32 y 33 mostrados en las Figuras 25 y 26, se puede observar que el 100% de los encuestados no cuenta con un procedimiento para el mantenimiento de equipos, dado que solo se revisan cuando existe el requerimiento, es por esto que se presenta incumplimiento del numeral A.11.2 (Equipos) del Anexo A de la norma ISO 27001:2013.

7.1.34 Resultado pregunta No. 34

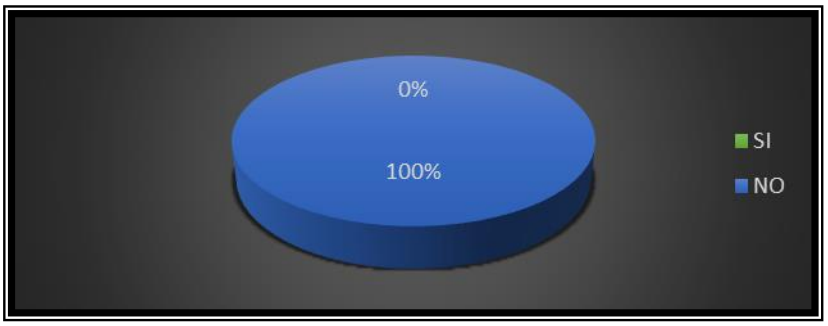
Figura 27. ¿Ha recibido capacitación o alguna formación acerca de riesgos informáticos a los que está expuesto?



Fuente. Los Autores

7.1.35 Resultado pregunta No. 35. Con qué frecuencia se realiza esta capacitación, como se obtuvo respuesta negativa en la pregunta anterior esta no aplica.

Figura 28. ¿Con que frecuencia se realiza esta capacitación?

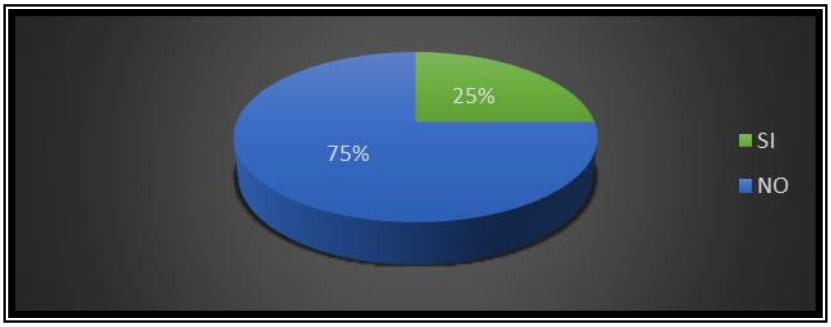


Fuente. Los Autores

En los resultados obtenidos en las preguntas 34 y 35 mostrados en las Figuras 27 y 28 donde el 100% de los encuestados indica que no ha recibido capacitación o formación en cuanto a los riesgos informáticos a los que están expuestos se evidencia incumplimiento de los numerales A.7 (Seguridad de los recursos humanos) y A.18 (Cumplimiento) del anexo A de la norma ISO 27001:2013.

7.1.36 Resultado pregunta No. 36

Figura 29. ¿La empresa permite guardar o consultar información personal en los equipos de la empresa o se tiene alguna limitación?



Fuente. Los Autores

7.1.37 Resultado pregunta No. 37

Cuadro 15. Tipos de Limitaciones

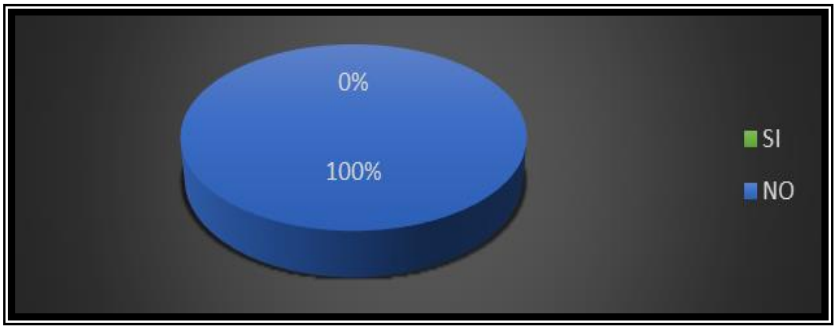
Encuesta	Respuesta
1.	No se permite guardar información personal.

Fuente. Los Autores

En los resultados de las preguntas 36 y 37 mostrados en la Figura 29 y Cuadro 15 donde el 75% de los encuestados indica que no se tienen limitaciones en cuanto al uso de información personal se evidencia incumplimiento de los numerales A.7 (Seguridad de los recursos humanos), A.9 (Control de acceso) y A.13 (Seguridad de las comunicaciones) del anexo A de la norma ISO 27001:2013.

7.1.38 Resultado pregunta No. 38

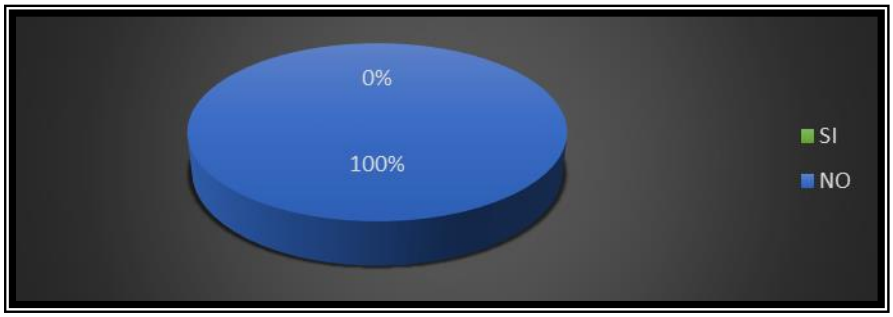
Figura 30. ¿El acceso a los recursos de red es restringido?



Fuente. Los Autores

7.1.39 Respuesta pregunta No. 39. De existir indique las restricciones, como se obtuvo respuesta negativa en la pregunta anterior esta no aplica.

Figura 31. De existir indique las restricciones



Fuente. Los Autores

En los resultados de las preguntas 38 y 39 mostrados en las Figuras 30 y 31 donde el 100% de los encuestados indica que no se tienen restricciones en los recursos de red podemos ver incumplimiento en los numerales A.9 (Control de acceso) y A.13 (Seguridad de las comunicaciones del anexo A de la norma ISO 27001:2013.

7.2 ANÁLISIS DE BRECHA ISO-27001

El análisis de brecha ISO 27001 en SISELCOM se realizó con la ayuda de la herramienta web de 27001 Academia, al cual se puede acceder desde el url https://advisera.com/27001academy/es/herramientas/herramienta-gratuita-analisis-de-brecha-para-iso-27001/.

El diagnóstico del estado actual con respecto al estado requerido por SISELCOM se realizó en dos fases; entrevista a gerencia con 110 preguntas relacionadas a cada uno de los controles de la norma y encuestas al personal con preguntas abiertas para tener más exactitud en cuanto a la percepción de seguridad.

Esta herramienta permite validar de manera fácil, cada uno de los controles y aspectos requeridos por la norma ISO 27001:2013.

7.2.1 Entrevista Gerencia

NOMBRE: Fernando Muñoz
CARGO: Gerente general

➢¿Existen políticas publicadas, aprobadas por la dirección, para apoyar la seguridad de la información?

Rta. No, pero se tienen contempladas.

➢¿Las políticas de seguridad de la información son revisadas y actualizadas?
Rta. No existen políticas de seguridad.

➢¿Están definidas todas las responsabilidades de seguridad de la información?

Rta. Si están definidas las funciones y responsabilidades en cuanto al manejo de la información.

➢¿Conoce la asignación de roles, responsabilidades y autoridades para la seguridad de la información?

Rta. Se tienen definidos los roles de acuerdo con el organigrama de la organización.

➢¿Las operaciones de la empresa se manejan dentro de un marco legal vigente y se mantiene contacto con las autoridades pertinentes?

Rta. Se mantienen todas las operaciones dentro del marco legal.

➢¿En la gestión de proyectos se consideran aspectos relacionados con la seguridad de la información?

Rta. Si, se firman contratos con cláusulas de manejo de información sobre todo con empresas públicas. En empresas privadas en algunos contratos.

➢¿Existen reglas para el manejo seguro de los dispositivos móviles?

Rta. Se manejan 2 equipos móviles dentro de la empresa, pero no se tienen reglas para el manejo de estos dispositivos. No se realiza revisión del manejo de estos dispositivos.

➢¿Existen reglas que definen cómo está protegida la información de la organización teniendo en cuenta el teletrabajo?

Rta. Se manejan 4 computadores de los cuales solo una persona puede realizar teletrabajo, pero no se manejan reglas para la protección de la información, no se realiza seguimiento. En el contrato se firma cláusula para el manejo de estos equipos.

➢¿La organización realiza verificaciones de antecedentes de los candidatos para el empleo o para los contratistas?

Rta. No, porque la mayoría de los empleados son referenciados o conocidos.

➢¿Existen acuerdos con los empleados y contratistas donde se especifiquen las responsabilidades de seguridad de información?

Rta. No.

➢¿La dirección exige que todos los empleados y contratistas cumplan con las reglas de seguridad de la información?

Rta. No, con los contratistas no se tiene control, pero solo conocen la información necesaria de la empresa.

➢¿Los empleados y contratistas reciben formación en toma de conciencia acerca del manejo de la seguridad de la información, y existen programas de sensibilización?

Rta. No.

➢¿La organización tiene un proceso disciplinario en caso de que se cometa una violación de seguridad?

Rta. No hay protocolo, pero a futuro se tiene la idea de un reglamento interno de trabajo.

➢¿Existen acuerdos que cubren las responsabilidades de seguridad de información que siguen siendo válidas después de la terminación del empleo?

Rta. Si, hasta 24 meses después de terminado el contrato según clausula.

➢¿Existe un inventario de activos?

Rta. Si.

➢¿Todos los activos en el inventario de activos tienen un dueño designado?

Rta. Si.

➢¿Existen definidas reglas para el manejo de activos y de información?

Rta. Si, en el contrato de arrendamiento de los equipos se manejan reglas de manejo y los equipos que se encuentran dentro de la organización están a cargo de la gerencia.

➢¿Los activos de la organización son devueltos cuando los empleados y contratistas finalizan su contrato?

Rta. Sí, pero no existe formato de entrega de equipos.

➢¿Existen procedimientos que definen cómo clasificar y manejar información clasificada?

Rta. No existe un procedimiento.

➢¿Existen procedimientos que definen cómo manejar activos?

Rta. No existen procedimientos escritos. Pero se conoce el manejo por parte de los trabajadores.

➢¿Existen procedimientos formales para la gestión de medios removibles?

Rta. No.

➢¿Son protegidos los medios que contienen información sensible durante contra el acceso no autorizado o modificación en su transporte?

Rta. Información sensible (Información bancaria, precios, cotizaciones, bases de datos de cliente y proveedores), no hay protección de los medios.

➢¿Existe una política de control de acceso?

Rta. No.

➢¿Los trabajadores tienen acceso sólo a los recursos que se les permite?

Rta. Si, solo tienen acceso a lo que necesitan.

➢¿Los derechos de acceso son proporcionados mediante un proceso de registro formal?

Rta. No.

➢¿Existe un sistema de control de acceso formal para el inicio de sesión en sistemas de información?

Rta. No.

➢¿Los derechos de acceso privilegiado son manejados con especial cuidado?

Rta. No.

➢¿Las contraseñas, y otra información de autenticación secreta, es proporcionada de forma segura?

Rta. No.

➢¿Los propietarios de activos comprueban periódicamente todos los derechos de acceso privilegiado?

Rta. No.

➢¿Los derechos de acceso son actualizados cuando hay un cambio en la situación del usuario (por ejemplo: cambio organizacional o terminación)?

Rta. Si.

➢¿Existen reglas para los usuarios sobre cómo proteger las contraseñas y otra información de autenticación?

Rta. No.

➢¿El acceso a la información en los sistemas es restringido según la política de control de acceso?

Rta. No.

➢¿Es requerido un sistema de login en los sistemas según la política de control de acceso?

Rta. No.

➢¿Los sistemas de gestión de contraseñas utilizados por los usuarios de la organización les ayuda a manejar de forma segura su información de autenticación?

Rta. No.

➢¿El uso de herramientas de utilidad es controlado y limitado a empleados específicos?

Rta. Si, cada empleado maneja únicamente las herramientas que necesita.

➢¿El acceso al código fuente es restringido a personas autorizadas?

Rta. No.

➢¿Existe una política para regular la encriptación y existen otros controles criptográficos?

Rta. No.

➢¿Están debidamente protegidas las claves criptográficas?

Rta. No hay claves criptográficas.

➢¿Existen zonas seguras que protegen la información sensible?

Rta. Si.

➢¿Es protegida la entrada a las zonas seguras?

Rta. No.

➢¿Las zonas seguras están ubicadas en un lugar protegido?

Rta. No.

➢¿Existen instaladas alarmas, sistemas de protección contra incendios y otros Sistemas?

Rta. No.

➢¿Existen definidos procedimientos para las zonas seguras?

Rta. No.

➢¿Las zonas entrega y carga están protegidas?

Rta. Solo se maneja una única puerta con seguridad.

➢¿Los equipos son debidamente protegidos?

Rta. No están ubicados en zona segura.

➢¿Los equipos están protegidos contra las variaciones de energía?

Rta. Si.

➢¿Están adecuadamente protegidos los cables de energía y telecomunicaciones?

Rta. Si.

➢¿Existe mantenimiento de los equipos?

Rta. Si, los que alquilan cada vez que vuelven a la empresa, computadores cada 6 meses.

➢¿La retirada de información y equipos fuera de la empresa está controlada?

Rta. No.

➢¿Los activos de la empresa son debidamente protegidos cuando no están en las instalaciones de la organización?

Rta. Si, están amparados bajo el contrato. Con los contratistas no hay nada firmado.

➢¿Es correctamente eliminada la información de los equipos que se van a eliminar o reutilizar?

Rta. Si.

➢¿Existen reglas para proteger los equipos cuando estos no estén siendo usados por los usuarios?

Rta. No.

➢¿Hay orientaciones a los usuarios sobre qué hacer cuando estos no están presentes en sus estaciones de trabajo?

Rta. No.

➢¿Están documentados los procedimientos de TI?

Rta. Se están documentando en el momento.

➢¿Los cambios que podrían afectar a la seguridad de la información son estrictamente controlados?

Rta. Si están controlados.

- ¿Los recursos son monitoreados y se realizan planes para asegurar su capacidad para cumplir con la demanda de los usuarios?

Rta. No.

- ¿Se separan los entornos de desarrollo, pruebas y producción?

Rta. El desarrollo es tercerizado.

- ¿El software antivirus y otros programas para la protección de malware se instalan y utilizan correctamente?

Rta. Todos los equipos están protegidos con defender.

- ¿Existe una política de backup definida y se lleva a cabo correctamente?

Rta. No.

- ¿Los eventos relevantes de los sistemas son verificados periódicamente?

Rta. No se revisa cada vez que falla.

- ¿Los registros están protegidos adecuadamente?

Rta. No.

- ¿Están adecuadamente protegidos los logs de los administradores?

Rta. El desarrollo es tercerizado.

- ¿Está la hora de todos los sistemas de TI sincronizada?

Rta. No.

- ¿La instalación de software es estrictamente controlada?

Rta. No.

- ¿La información de análisis de vulnerabilidades es correctamente gestionada?

Rta. No.

➢¿Existen reglas para definir restricciones de instalación de software a los usuarios?

Rta. No.

➢¿Existen auditorias donde se realice verificación de los sistemas operativos?

Rta. No.

➢¿Las redes son gestionadas para proteger la información de sistemas y aplicaciones?

Rta. No.

➢¿Los requisitos de seguridad para servicios de red están incluidas en los acuerdos?

Rta. Tercerizado.

➢¿Existen redes segregadas considerando los riesgos y la clasificación de los activos?

Rta. Si.

➢¿Las transferencias de información están debidamente protegidas?

Rta. No.

➢¿Los acuerdos con terceras partes consideran la seguridad durante la transferencia de información?

Rta. Algunas veces con algunas empresas cláusulas de seguridad de la información.

➢¿Los mensajes que se intercambian sobre las redes están protegidos correctamente?

Rta. No.

➢¿La organización posee una lista con todas las cláusulas de confidencialidad que deben ser incluidos en los acuerdos con terceros?

Rta. No.

➢¿Se definen requisitos de seguridad para nuevos sistemas de información, o para cualquier cambio sobre ellos?

Rta. No.

➢¿La información de aplicaciones transferida a través de redes públicas es adecuadamente protegida?

Rta. No.

➢¿Las transacciones de información a través de redes públicas son adecuadamente protegidas?

Rta. No.

➢¿Existen definidas reglas para el desarrollo seguro de software y de los sistemas?

Rta. Se realiza la verificación a la empresa que realiza el desarrollo.

➢¿Se controlan los cambios en los sistemas nuevos o existentes?

Rta. No.

➢¿Las aplicaciones críticas son debidamente probadas después de los cambios realizados en los sistemas operativos?

Rta. No.

➢¿Se realizan sólo los cambios necesarios a los sistemas de información?

Rta. No.

➢Los principios de ingeniería de sistemas seguros son aplicados al proceso de desarrollo de sistemas de la organización?

Rta. El desarrollo es tercerizado.

➢¿Es seguro el entorno de desarrollo?

Rta. Es tercerizado.

➢¿Es monitorizado el desarrollo externalizado de sistemas?

Rta. Si.

- ¿Existe definido un criterio para aceptar los sistemas?

Rta. No.

- ¿Los datos de prueba son cuidadosamente seleccionados y protegidos?

Rta. No.

- ¿Existe una política para el tratamiento de los riesgos relacionados con proveedores?

Rta. No.

- ¿Los requisitos de seguridad son incluidos en los acuerdos con los proveedores?

Rta. No.

- ¿Los acuerdos con los proveedores incluyen requisitos de seguridad?

Rta. No.

- ¿Son supervisados regularmente los proveedores?

Rta. Sí, pero no están documentados.

- ¿Los cambios relacionados con los acuerdos y contratos con proveedores tienen en cuenta los riesgos existentes?

Rta. No.

- ¿Los incidentes son gestionados adecuadamente?

Rta. Solo se han presentado robos, con reporte a las autoridades.

- ¿Los eventos de seguridad son reportados adecuadamente?

Rta. No se han presentado.

- ¿Los empleados y contratistas informan sobre las debilidades de seguridad?

Rta. Los empleados informan, pero sin formato.

➢¿Los eventos de seguridad son evaluados y clasificados correctamente?

Rta. No.

➢¿Están documentados los procedimientos para dar respuesta a los incidentes?

Rta. No hay procedimientos.

➢¿Se analizan los incidentes de seguridad correctamente?

Rta. No.

➢¿Existen procedimientos que definen cómo recopilar evidencias?

Rta. No.

➢¿Existen definidos requisitos para la continuidad de la seguridad de la información?

Rta. No.

➢¿Existen procedimientos que aseguren la continuidad de la seguridad de la información durante una crisis o un desastre?

Rta. No.

➢¿Se realizan test y pruebas de continuidad?

Rta. No.

➢¿La infraestructura IT está redundada, incluyendo su planeamiento y operación?

Rta. No.

➢¿Son conocidos los requisitos legislativos, regulatorios, contractuales y cualquier otro requisito relativo a seguridad?

Rta. No.

➢¿Existen procedimientos para proteger los derechos de propiedad intelectual?

Rta Si existen clausulas en los contratos.

➢¿Los registros están protegidos adecuadamente?

Rta. No.

- ¿La información personal está protegida adecuadamente?

Rta. No.

- ¿Se utilizan controles criptográficos correctamente?

Rta. No.

- ¿La seguridad de la información es revisada regularmente por un auditor independiente?

Rta. No.

- ¿Los gerentes revisan regularmente si las políticas de seguridad y procedimientos son llevadas a cabo adecuadamente en sus áreas de responsabilidad?

Rta. No.

- ¿Los sistemas de información son revisados regularmente para comprobar su cumplimiento con los estándares y las políticas de seguridad de la información?

Rta. No.

Terminada la entrevista con el gerente de la empresa se consolida la información, comparando las respuestas de los diferentes entrevistados y acercando más a la realidad la situación actual de la empresa, a continuación, se describe el resultado general del análisis de brecha.

7.2.2 Análisis de brecha. En este analisis se pueden identificar las amenazas que exponen la confidencialidad, integridad y disponibilidad de la información, por consiguiente, se evalúan los controles que se están implementando en la empresa y se diagnostica su estado actual frente a la seguridad.

A partir del análisis que se realice posterior a la obtención de los resultados, se dará a conocer el estado actual de la empresa respecto al cumplimento de los requisitos y controles definidos por la norma ISO27001:2013 para el diseño de un sistema de gestión de seguridad de la información y las acciones y recursos que serán requeridos para lograr el cumplimiento del estado al que se desea llegar partiendo del estado en el que se encuentra actualmente la empresa.

Dentro de este análisis se establecen en el Cuadro 16 las zonas para identificar en qué estado de cumplimiento se encuentra la empresa con respecto a la norma ISO 27001:2013.

Cuadro 16. Valoración de controles

Valoración de controles	
NO CUMPLIDO	La empresa no cumple con el control.
EN PROCESO DE IMPLEMENTACIÓN	La empresa se encuentra en el proceso de implementación del control.
CUMPLIDO	La empresa cumple al 100% con el control.

Fuente. Los Autores

El análisis de brecha se realiza como parte de la identificación del estado actual del cumplimiento la empresa SISELCOM S.A.S., en cuanto a la seguridad de la información, el análisis se realizó con respecto a los requisitos y controles descritos en el anexo A de la norma ISO 27001:2013, este ayudará a determinar el estado actual y el estado al que se quiere llegar se muestra en el Cuadro 17.

Cuadro 17. Análisis aplicabilidad de la norma ISO 27001-2013

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
A. 5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Ni la gerencia ni los empleados conocen los riesgos que se tienen en cuanto a la seguridad de la información.	Incumplimiento en todos los puntos de la norma ya que sin políticas no es posible contar con una buena seguridad en la información.	Políticas para la seguridad de la información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	Gerencia	NO CUMPLIDO
	No se tiene conocimiento de la importancia de la seguridad de la información.	Falta de conciencia en cuanto a la seguridad de la información, mayor vulnerabilidad para el negocio.	Revisión de las políticas para la seguridad de la información. Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	Gerencia	NO CUMPLIDO
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	La gerencia tiene clara la asignación de roles y responsabilidades pero los empleados no lo tienen claro.	Mal manejo de la información por parte del personal.	Roles y responsabilidades para la seguridad de la información. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Gerencia	EN PROCESO DE IMPLEMENTACIÓN

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	Actualmente las responsabilidades están definidas pero se observa desinformación por parte del personal.	Posible pérdida de información.	Separación de deberes. Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	Gerencia	EN PROCESO DE IMPLEMENTACIÓN
	Las operaciones se manejan dentro del marco legal vigente.	Cumplido	Contacto con las autoridades. Se deben mantener contactos apropiados con las autoridades pertinentes.	Gerencia	CUMPLIDO
	No se evidencia contacto con autoridades pertinentes.	Desconocimiento de temas asociados al tema de seguridad ya que no existe un medio para retroalimentar fallas.	Contacto con grupos de interés especial. Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	Gerencia	NO CUMPLIDO
	Si me tiene en cuenta la seguridad de la información en la gestión de proyectos.	Cumplido	Seguridad de la información en la gestión de proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	Gerencia	CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	Acceso de dispositivos móviles sin restricción.	Altos riesgos inducidos por uso de dispositivos móviles.	Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Gerencia	NO CUMPLIDO
	No se evidencia una política y medidas de seguridad para salvaguardar la información.	Pérdida de información vulnerable, riesgo en cuanto a la imagen empresarial.	Teletrabajo. Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada y almacenada en los lugares en los que se realiza teletrabajo.	Gerencia	NO CUMPLIDO
A. 7 SEGURIDAD DE LOS RECURSOS HUMANOS	No se realiza el proceso de estudio para el personal que labora.	Posible robo de información, riesgo en cuanto al personal que maneja información sensible de la organización.	Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	Con los empleados se tienen acuerdos contractuales, pero con los contratistas en algunos casos no.	Extracción de información correspondiente al nivel de clasificación de la información	Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	Gerencia	EN PROCESO DE IMPLEMENTACIÓN
	Sobre los contratistas no se tiene control y no se exige la aplicación de la seguridad de la información.	Posible pérdida de información, mala imagen de la empresa hacia el exterior.	Responsabilidades de la dirección. La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	Gerencia	NO CUMPLIDO
	Falta de capacitación para el personal que hace parte de los procesos.	Desconocimiento del personal en cuanto a los riesgos a los que están expuestos, posible pérdida o daño de información.	Toma de conciencia, educación y formación en la seguridad de la información. Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimiento de la organización pertinentes para su cargo.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se cuenta con un proceso disciplinario o conocimiento de acciones formales.	Desconocimiento de la ley y de las posibles consecuencias a una violación de la seguridad de la información.	Proceso disciplinario. Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Gerencia	NO CUMPLIDO
	No se evidencia la existencia proceso y/o métodos para informar la terminación o cambio de responsabilidad de empleo.	No hay compromiso ni responsabilidad del empleado.	Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Gerencia	NO CUMPLIDO
A 8. GESTIÓN DE ACTIVOS	Si hay inventario de activos	Cumplido	Inventario de activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	Gerencia	CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	Si tienen asignado propietario los activos.	Cumplido	Propiedad de los activos. Los activos mantenidos en el inventario deben tener un propietario.	Gerencia	CUMPLIDO
	Si se hace uso aceptable de activos.	Cumplido	Uso aceptable de los activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Gerencia	CUMPLIDO
	No se evidencia la existencia de un proceso formal de devolución de activos de empleados o contratistas.	Difícil trazabilidad de los activos - aumento de las necesidades tecnológicas - Pérdida de información.	Devolución de activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Gerencia	NO CUMPLIDO
	No se evidencia clasificación de la información.	Divulgación de información por personal no autorizado.	Clasificación de la información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se cuenta con un proceso de etiquetado de información.	Posible pérdida de información, no se tiene claro el nivel de importancia de la información.	Etiquetado de la información. Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Gerencia	NO CUMPLIDO
	No se tiene documentado un proceso para el manejo adecuado de activos.	Posible daño o pérdida de activos.	Manejo de activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Gerencia	NO CUMPLIDO
	No se evidencia un tratamiento para los medios de soporte removibles.	Fuga de información - Pérdida de datos.	Gestión de medios removibles. Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Gerencia	NO CUMPLIDO
	No se evidencia un mecanismo para la disposición de los medios de soporte.	Fuga de información - falta de control de los activos.	Disposición de los medios. Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia de un proceso para la transferencia de medios de soporte físicos.	Fuga de información - uso mal intencionado.	Transferencia de medios físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Gerencia	NO CUMPLIDO
A. 9 CONTROL DE ACCESO	No existe política control de acceso.	Desconocimiento una política de control acceso por parte del personal.	Política de control de acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Gerencia	NO CUMPLIDO
	No se evidencia control de acceso a la red y a los servicios.	Ingreso personal no autorizado - manipulación inadecuada de la información y los servicios.	Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Gerencia	NO CUMPLIDO
	No se evidencia control del registro y cancelación de usuarios.	Ingreso personal no autorizado - manipulación inadecuada de la información y los servicios.	Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia un mecanismo para el suministro de acceso a los usuarios.	Posible fuga de información.	Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para los sistemas y servicios.	Gerencia	NO CUMPLIDO
	No se evidencia un mecanismo para el suministro de acceso a los usuarios.	Uso inadecuado de la información.	Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Gerencia	NO CUMPLIDO
	No existe asignación de información de autenticación secreta.	Posible robo de información.	Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Gerencia	NO CUMPLIDO
	No se evidencia la existencia de revisiones periódicas de acceso de los usuarios.	Accesos sin control. Fuga de información.	Revisión de los derechos de acceso de usuarios. Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	Si se hacen ajustes de derechos de acceso al terminar el empleo.	Cumplido	Retiro o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Gerencia	CUMPLIDO
	Desconocimiento de información secreta y el cuidado que deben tener los empleados con esta información.	Mala manipulación y posible divulgación de la información.	Uso de información de autenticación secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Gerencia	NO CUMPLIDO
	No se evidencia restricción de acceso a la información.	Acceso no autorizado - modificación en la documentación.	Restricción de acceso a la información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia la existencia de un procedimiento de ingreso seguro.	Fuga o pérdida de información en la transferencia.	Procedimiento de ingreso seguro. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Gerencia	NO CUMPLIDO
	No se evidencia un procedimiento de gestión de contraseñas.	Ingreso no autorizado a información, contraseñas no seguras.	Sistema de gestión de contraseñas. Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Gerencia	NO CUMPLIDO
	No se evidencia el control sobre programas utilitarios.	Posible pérdida de información, denegación de servicio.	Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Gerencia	NO CUMPLIDO
	No se evidencia un procedimiento para el control de acceso al código fuente.	Modificación de información - acceso no autorizado.	Control de acceso a códigos fuente de programas. Se debe restringir el acceso a los códigos fuente de los programas.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
A. 10 CRIPTOGRAFÍA	No se evidencia la existencia de una política que aplique los controles criptográficos.	Posible pérdida de información sobre todo en lo equipos utilizados en teletrabajo.	Política sobre el uso de controles criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Gerencia	NO CUMPLIDO
	No se evidencia la existencia de un procedimiento de gestión de claves.	Divulgación de la información sin control.	Gestión de llaves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	Gerencia	NO CUMPLIDO
A. 11 SEGURIDAD FÍSICA Y DEL ENTORNO	No se evidencia la delimitación de perímetro de seguridad.	Posible robo o pérdida de información- Robo a daño de activos.	Perímetro de seguridad física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	Gerencia	NO CUMPLIDO
	La empresa no cuenta con controles de entrada físicos para el personal o visitantes.	Fuga de información- alteración en las operaciones - acceso no autorizado - vandalismo.	Controles de acceso físicos. Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	La empresa no cuenta con separación de oficinas ni con controles de acceso.	Fuga de información- alteración en las operaciones - acceso no autorizado - vandalismo.	Seguridad de oficinas, recintos e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	Gerencia	NO CUMPLIDO
	No se evidencia la existencia de un procedimiento contra las amenazas ambientales.	Perdida de información - Daño de activos.	Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Gerencia	NO CUMPLIDO
	No se evidencia que se tome en cuenta el tema de trabajo en áreas seguras.	Perdida o fuga de información.	Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Gerencia	NO CUMPLIDO
	No se cuenta con protección en el área de carga y despacho.	Posible daño o pérdida de activos.	Áreas de despacho y carga. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	Los equipos como ups o baterías que se encuentran en la empresa no se encuentran ubicados de manera adecuada.	Daño o pérdida de activos.	Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Gerencia	NO CUMPLIDO
	Los equipos se encuentran protegidos.	Cumplido	Servicios de suministro. Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Gerencia	CUMPLIDO
	El cableado se encuentra protegido.	Cumplido	Seguridad del cableado. El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	Gerencia	CUMPLIDO
	No se tiene documentación o procedimiento de mantenimiento de equipos.	Daño de equipos o activos, daño o perdida de información.	Mantenimiento de equipos. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se encuentra con un procedimiento de retiro de activos.	Perdida de activos, falta de control en los activos.	Retiro de activos. Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	Gerencia	NO CUMPLIDO
	Con los contratistas no se tienen contratos que aseguren los activos mientras están en su poder.	Perdida de activos, daño de activos.	Seguridad de equipos y activos fuera de las instalaciones. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Gerencia	NO CUMPLIDO
	Los equipos son verificados.	Cumplido	Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	Gerencia	CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No existen reglas para proteger los equipos cuando no son usados por los usuarios.	Robo o pérdida de información.	Equipos de usuario desatendido. Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	Gerencia	NO CUMPLIDO
	No se evidencia procedimiento para tratar la política de escritorio limpio y pantalla limpia.	Información vulnerable - fuga y Pérdida de información	Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	Gerencia	NO CUMPLIDO
A. 12 SEGURIDAD DE LAS OPERACIONES	Los procedimientos se encuentran en proceso de documentación.	Errores al realizar procedimientos, mal manejo de información.	Procedimientos de operación documentados. Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que lo necesitan.	Gerencia	EN PROCESO DE IMPLEMENTACIÓN
	No se evidencia proceso de gestión de cambios dentro de la empresa.	Por la falta de planeamiento metodológico se puede incurrir en fallas constantes.	Gestión de cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia gestión de capacidad.	No se cuenta con información acerca de las proyecciones requeridas al sistema.	Gestión de capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura para asegurar el desempeño requerido del sistema.	Gerencia	NO CUMPLIDO
	No se cuenta con separación de ambientes en la empresa.	Acceso no autorizado tanto físico como en la información.	Separación de los ambientes de desarrollo, pruebas y operación. Se deben separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Gerencia	NO CUMPLIDO
	Los empleados no cuentan con capacitación en cuanto a los daños informáticos a los que están expuestos.	Virus - ejecución no autorizada de programas - intrusión a red interna.	Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se cuenta con un procedimiento de backups definido.	Perdida de información, daño en equipos por almacenamiento innecesario de información.	Respaldo de la información. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Gerencia	NO CUMPLIDO
	No se evidencia procedimiento documental para el manejo de los registros de eventos.	Perdida de trazabilidad de eventos.	Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Gerencia	NO CUMPLIDO
	No se evidencia algún proceso en la protección de la información.	Fuga de información.	Protección de la información de registro. Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Gerencia	NO CUMPLIDO
	No existen registros de operaciones.	Intrusión – pérdida de información.	Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se tiene sincronización de relojes en los equipos.	Modificación de operaciones.	Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	Gerencia	NO CUMPLIDO
	No se evidencia un procedimiento que bloquee instalación de software.	Introducción de virus, mal manejo de los sistemas.	Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Gerencia	NO CUMPLIDO
	No se cuenta con un análisis de riesgo, no se identifican adecuadamente las vulnerabilidades.	Mal manejo de los sistemas, fuga de información.	Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia la existencia de reglamento para la instalación de software.	Mal uso de los equipos, introducción de virus.	Restricciones sobre la instalación de software. Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Gerencia	NO CUMPLIDO
	No se evidencia de la existencia de auditorías sobre el sistema de información.	No existe planificación, ni control del sistema.	Controles de auditorías de sistemas de información. Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Gerencia	NO CUMPLIDO
A. 13 SEGURIDAD DE LAS COMUNICACIONES	No se evidencia control o gestión sobre las redes.	Sistemas inseguros, posible daño o pérdida de información.	Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	Gerencia	NO CUMPLIDO
	No se cuenta con mecanismos de seguridad sobre los servicios de red.	Fuga o daño de información.	Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	Se tiene segmentación de redes.	Cumplido	Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	Gerencia	CUMPLIDO
	No se evidencia ninguna política y procedimientos de transferencia de información.	Divulgación de información - Robo de información,	Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Gerencia	NO CUMPLIDO
	No se evidencia de la existencia de los acuerdos sobre transferencia de información.	Desconocimiento del riesgo informático.	Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	Gerencia	NO CUMPLIDO
	No se evidencia mecanismos documentados que permitan la protección de los mensajes electrónicos.	Fuga de información ingeniería social.	Mensajería electrónica. Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	Existen ciertos acuerdos de confidencialidad, pero algunos no se encuentran documentados.	Fuga de información.	Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	Gerencia	EN PROCESO DE IMPLEMENTACIÓN
A. 14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	No se evidencia la elaboración de análisis previos que contemplen los requisitos mínimos de la seguridad de la información para nuevos sistemas.	Fallas en seguridad al realizar cualquier cambio ya sea de sistemas o de equipos en la empresa.	Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	Gerencia	NO CUMPLIDO
	No se evidencia la aplicación de seguridad de servicios para la aplicación en redes públicas.	Pérdida o robo de información.	Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia procedimiento para la protección de transacciones de servicios de aplicaciones.	Mensajes no autorizados, fuga de información.	Protección de transacciones de los servicios de las aplicaciones. La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.	Gerencia	NO CUMPLIDO
	El desarrollo esta tercerizado.	Cumplido	Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.		CUMPLIDO
	No existen procedimientos de control de cambios.	Daño en los sistemas, perdida de información.	Procedimientos de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia la aplicación de un proceso de seguridad que revise las aplicaciones luego de los cambios.	Indisponibilidad del servicio - Pérdida de información.	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Gerencia	NO CUMPLIDO
	No se evidencian restricciones en los cambios de software.	Daño o pérdida de información.	Restricciones en los cambios a los paquetes de software. Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios y todos los cambios se deben controlar estrictamente.	Gerencia	NO CUMPLIDO
	No se cuentan con principios de construcción de sistemas seguros.	Mal uso de las herramientas.	Principios de construcción de los sistemas seguros. Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros y aplicarlos a cualquier actividad de implementación de sistemas de información.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	El desarrollo esta tercerizado.	Cumplido	Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	Gerencia	CUMPLIDO
	No se cuenta con un procedimiento documentado para supervisar el desarrollo externo.	Divulgación de la información confidencial-daño en imagen empresarial.	Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	Gerencia	NO CUMPLIDO
	No se evidencian pruebas de seguridad para la implementación de actividades de desarrollo subcontratadas.	Posibles fallas en el servicio.	Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia proceso para las pruebas de aceptación de sistemas.	Falta de trazabilidad en los sistemas, posibles fallas.	Prueba de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Gerencia	NO CUMPLIDO
	No se evidencia protección de datos de prueba.	No hay seguimiento de las pruebas que se deben realizar.	Protección de datos de prueba. Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Gerencia	NO CUMPLIDO
A. 15 RELACIONES CON LOS PROVEEDORES	No se evidencia el establecimiento de la política de seguridad de la información con los proveedores.	Perdida de información, daño en imagen empresarial.	Política de seguridad de la información para las relaciones con proveedores. Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencian acuerdos de seguridad de la información con los proveedores.	Perdida de activos o de información confidencial.	Tratamiento de la seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	Gerencia	NO CUMPLIDO
	No se cuenta con una cadena de suministro de tecnología de información con proveedores.	Perdida de información o de equipos, daño en la imagen empresarial.	Cadena de suministro de tecnología de información y comunicación. Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Gerencia	NO CUMPLIDO
	No se evidencia un procedimiento para auditar los servicios de los proveedores.	Posible modificación de información.	Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se cuenta con un procedimiento de gestión de cambios.	Daño en imagen empresarial.	Gestión de cambios en los servicios de los proveedores. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.	Gerencia	NO CUMPLIDO
A. 16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	No se evidencian procedimientos de gestión de incidentes.	Desconocimiento de los riesgos e incidentes.	Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
		Perdida de trazabilidad de eventos.	Reporte de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	Gerencia	NO CUMPLIDO
	No se evidencia la existencia de un proceso de retroalimentación de las debilidades de seguridad de la información.	No se realiza tratamiento a tiempo de las vulnerabilidades presentadas.	Reporte de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	Gerencia	NO CUMPLIDO
	No se evidencia evaluación de eventos de la seguridad de la información.	Desconocimiento de los eventos que se presentan en la empresa.	Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No existe evidencia de respuestas de incidentes de la seguridad de la información.	Daño en los sistemas, perdida de información.	Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Gerencia	NO CUMPLIDO
	No se aplica el conocimiento de los incidentes para mejorar la seguridad.	Desconocimiento del estado de seguridad y de los riesgos a los que está expuesta la empresa.	Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	Gerencia	NO CUMPLIDO
	No existe un procedimiento que salvaguarde la evidencia.	Perdida de evidencias por lo que no se podrían validar los incidentes de forma adecuada.	Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
A. 17 CONTINUIDAD DE NEGOCIO	No se evidencia planificación de la continuidad de la seguridad de la información.	Falta de documentación importante para el proceso de seguridad.	Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Gerencia	NO CUMPLIDO
	No se evidencian procedimientos ni controles que aseguren la información.	Posibles daños en los sistemas por no aplicar buenos procedimientos.	Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia que exista una verificación de los controles de la seguridad de la información.	No se identificarían los avances en cuanto a seguridad en la empresa.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Gerencia	NO CUMPLIDO
	No se evidencia existencia de mecanismos que aseguren la disponibilidad del procesamiento de información.	Negación de servicio	Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
A. 18 CUMPLIMIENTO	No se tiene totalmente identificada la legislación aplicable.	Desconocimiento de las responsabilidades legales.	Identificación de la legislación aplicable y de los requisitos contractuales. Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Gerencia	NO CUMPLIDO
	Si se manejan clausulas en los contratos de propiedad intelectual.	Cumplido	Derechos de propiedad intelectual. Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Gerencia	CUMPLIDO
	No se evidencia un procedimiento para la protección de registros.	Modificación de información - acceso no autorizado.	Protección de registros. Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia que se asegure la privacidad y protección de la información personal.	Posible modificación de información.	Privacidad y protección de información de datos personales. Se deben asegurar la privacidad y la protección de la información de datos personales como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	Gerencia	NO CUMPLIDO
	No se evidencia de la aplicación de mecanismo que encripte la información de la entidad bajo los parámetros establecidos.	Divulgación o pérdida de información.	Reglamentación de controles criptográficos. Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Gerencia	NO CUMPLIDO
	No se evidencia la revisión independiente de la seguridad cuando ocurren cambios significativos.	Des aseguramiento de la información.	Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	Gerencia	NO CUMPLIDO

Cuadro 17. (Continuación)

Numeral norma	Descripción de la vulnerabilidad	Consecuencia	Control	Responsable	Valoración de controles
	No se evidencia el cumplimiento y seguimiento de las políticas y normas de seguridad.	Des aseguramiento de la información.	Cumplimiento con las políticas y normas de seguridad. Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.	Gerencia	NO CUMPLIDO
	No se evidencia que se realice una revisión del cumplimiento técnico.	Incremento en fallas técnicas.	Revisión del cumplimiento técnico. Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	Gerencia	NO CUMPLIDO

Fuente. Los Autores

7.3 CONSOLIDADO DE CUMPLIMIENTO DE CONTROLES DE LA NORMA ISO 27001:2013

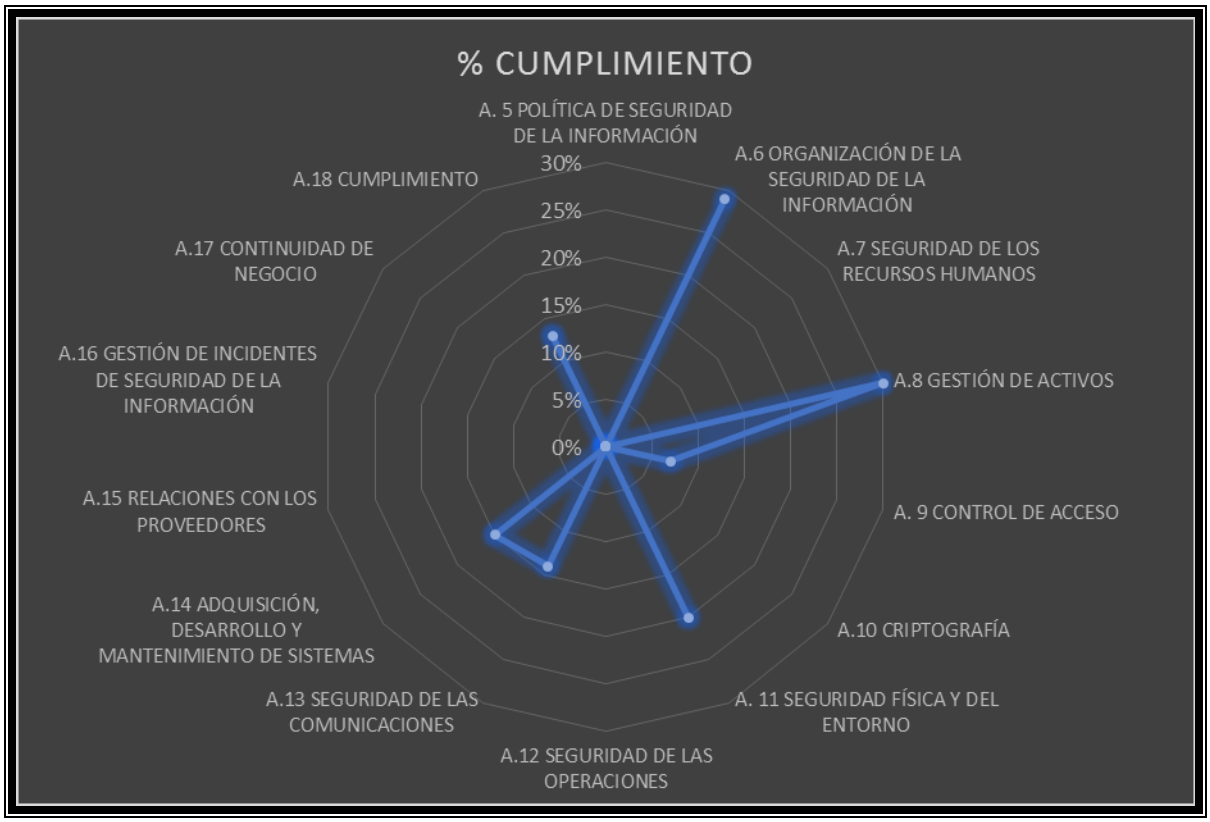
De acuerdo al análisis de brecha realizado y las zonas de riesgo establecidas se obtuvo el nivel de cumplimiento de los controles del anexo A de la norma ISO 27001:2013 mostrados en el Cuadro 18:

Cuadro 18. Consolidado cumplimiento de controles

Control	Total	Cumplidos	% cumplimiento	% incumplimiento
A. 5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	2	0	0%	100%
A. 6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	7	2	29%	71%
A. 7 SEGURIDAD DE LOS RECURSOS HUMANOS	6	0	0%	100%
A. 8 GESTIÓN DE ACTIVOS	10	3	30%	70%
A. 9 CONTROL DE ACCESO	14	1	7%	93%
A. 10 CRIPTOGRAFÍA	2	0	0%	100%
A. 11 SEGURIDAD FÍSICA Y DEL ENTORNO	15	3	20%	80%
A. 12 SEGURIDAD DE LAS OPERACIONES	14	0	0%	100%
A. 13 SEGURIDAD DE LAS COMUNICACIONES	7	1	14%	86%
A. 14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	13	2	15%	85%
A. 15 RELACIONES CON LOS PROVEEDORES	5	0	0%	100%
A. 16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	7	0	0%	100%
A. 17 CONTINUIDAD DE NEGOCIO	4	0	0%	100%
A. 18 CUMPLIMIENTO	8	1	13%	88%
TOTAL	114	13	11%	89%

Fuente. Los Autores

Figura 32. Gráfica cumplimiento controles

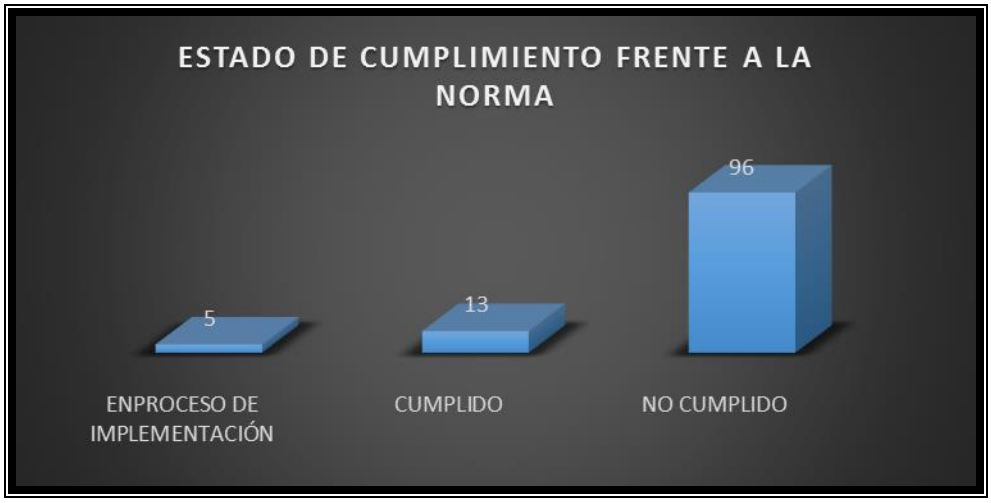


Fuente. Los Autores

En el Cuadro 18 esta dispuesto el total de controles que contiene el anexo A de la norma ISO 27001:2013 y el total de controles cumplidos por la empresa, con una regla de 3 se calcula tanto el porcentaje de cumplimiento como él porcentaje de incumplimiento de los controles.

En la Figura 32 se encuentra plasmado gráficamente el porcentaje de cumplimiento de cada uno de los numerales de la norma. Con lo anterior se evidencia que la empresa se encuentra en un porcentaje de cumplimiento del 11% y en los numerales A. 8 Gestión de activos y A. 6 Organización de la seguridad de la información con un 30% y un 29% respectivamente son los de mayor cumplimiento lo brinda para la empresa una acción de satisfacción en el nivel de cumplimento a la norma, según entrevistas con la gerencia en el momento lo más importante es el cuidado de los activos ya que el mayor ingreso proviene del alquiler de equipos por lo que se da prioridad al cuidado de los mismos.

Figura 33. Estado de cumplimiento



Fuente. Los Autores

En el proceso de calificación en la Figura 33, podemos ver que la empresa se encuentra solo en un 11% de cumplimiento frente a la norma, lo que representa un riesgo alto para la misma.

7.4 ANÁLISIS CONTEXTO DE SEGURIDAD

En la actualidad SISELCOM no cuenta con un sistema de gestión de seguridad de la Información documentado e implementado, el resultado del análisis de brecha muestra en su gran mayoría incumplimiento en cada uno de los controles evaluados con respecto a la norma ISO 27001:2013. Lo anterior no quiere decir que SISELCOM no tenga en cuenta la seguridad de la información en sus procesos, al momento de realizar el análisis cumplen algunos controles y otros no están debidamente documentados, pero se realizan, lo que ayuda a minimizar riesgos en la seguridad de sus activos.

Actualmente SISELCOM se encuentra trabajando en la documentación de los procesos y procedimientos en cada una de las áreas de la compañía, esto se realiza como parte del compromiso de buscar la certificación de sistema de seguridad y salud en el trabajo, sin embargo el hecho de que los procesos y procedimientos no estén totalmente documentados permite que se abra la oportunidad para cometer errores en la ejecución de las actividades diarias, adicional la falta de entrenamiento en seguridad de la información al personal permite que el recurso humano sea susceptible a amenazas tales como ingeniería social y phishing.

7.4.1 Mapa de procesos. Dentro del diseño del sistema de gestión de calidad que se encuentra en proceso de implementación con base en la norma ISO

9001:2015 dentro de la empresa SISELCOM S.A.S. Se plantea el mapa de procesos de información que están dentro del alcance de este proyecto en la Figura 34:

7.4.1.1 Procesos operativos. Los procesos operativos se definen como aquellos procesos que se encuentran directamente ligados a la realización del producto y/o la prestación del servicio. Por ello se conocen como los procesos de "línea".

Dichos procesos cuentan con una visión completa del cliente, desde el conocimiento de los requisitos del producto o servicio, hasta el análisis final de satisfacción, una vez el cliente ha recibido nuestro producto o servicio.

Para nuestro caso aplican los siguientes procesos:

- Ventas y mercadeo.
- Formulación y ejecución de proyectos.
- Servicio técnico y mantenimiento de equipos.

7.4.1.2 Procesos estratégicos. Los procesos estratégicos se definen como aquellos procesos que se encuentra directamente vinculados al ámbito de las responsabilidades de la dirección y, generalmente, al largo plazo. Se refiere principalmente a procesos de planificación y otros procesos que se encuentren ligados a factores clave o factores estratégicos.

Los procesos estratégicos conducen a los operativos mediante pautas de gestión o estratégicas, y los procesos de apoyo colaboran en su desarrollo.
En nuestro caso aplican los siguientes procesos:

- Contratación de personal.
- Procesos gerenciales.

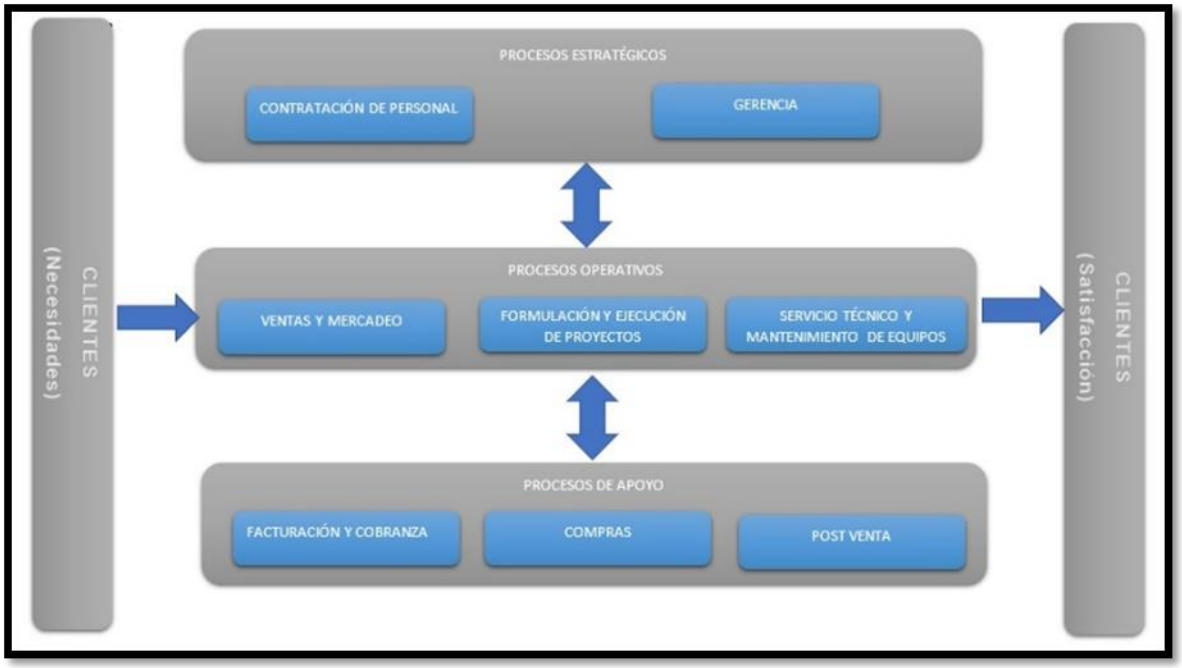
7.4.1.3 Procesos de soporte. Los procesos de soporte se definen como aquellos procesos que ofrecen soporte a los procesos operativos. Se refiere principalmente a procesos relacionados con recursos y mediciones.

Una de las principales características de los procesos de apoyo es que pueden ser fácilmente subcontratables, es decir, que la empresa no se resiente en el momento en que se opta por externalizar alguna de las tareas o actividades que se llevan a cabo en los procesos de apoyo.

Para la empresa aplican los siguientes procesos:

- Facturación y cobranza.
- Compras.
- Postventa.

Figura 34. Mapa de procesos SISELCOM



Fuente. Los Autores

7.4.2 Definición de procedimientos. En la verificación de la documentación de SISELCOM S.A.S. y con ayuda de la gerencia se definen los siguientes procedimientos que actualmente se encuentran en proceso de documentación bajo el estándar de la norma ISO 9001:2015:

7.4.2.1 Procedimiento de facturación y cobranza.

➢**Objetivo:** establecer los lineamientos y pasos necesarios para la emisión, recepción y contabilización de facturas y cuentas de cobro tanto a proveedores como clientes de la empresa, así como las gestiones administrativas de cobranza de la cartera.

➢**Alcance:** aplicable al proceso de facturación y cobranzas de SISELCOM S.A.S.

➢**Responsables:** Charly Rocha y Andrea Camargo.

7.4.2.2 Procedimiento de compras.

➢**Objetivo:** el procedimiento tiene como objetivo establecer los lineamientos necesarios para realizar la compra de productos y/o servicios críticos para la empresa, así como la consecución de nuevos proveedores.

➢**Alcance:** se tiene contemplado un alcance desde la cotización del producto o servicio hasta el pago y entrega del mismo.

➢**Responsables:** Fernando Muñoz y Charly Rocha

7.4.2.3 Procedimiento de ventas y mercadeo.

➢**Objetivo:** el objetivo de este procedimiento es definir la metodología de contacto con los clientes existentes y clientes potenciales.

➢**Alcance:** se incluye la presentación comercial de los productos, la oferta comercial y la creación del cliente en el sistema contable para su posterior facturación.

➢**Responsables:** Fernando Muñoz, Johana Matiz y Julián Orjuela.

7.4.2.4 Procedimiento postventa.

➢**Objetivo:** el procedimiento tiene como objetivo establecer el método de prestación del servicio de postventa.

➢**Alcance:** cubre desde la garantía de equipos o servicios, la generación reporte técnico y cualquier soporte que solicite el cliente.

➢**Responsables:** Fernando Muñoz y Julián Orjuela.

7.4.2.5 Procedimiento de contratación del personal.

➢**Objetivo:** en este procedimiento se define el proceso de contratación tanto del personal contratista como directo de la empresa.

➢**Alcance:** incluye la verificación de referencias, antecedentes y revisión del contrato.

➢**Responsables:** Fernando Muñoz.

7.4.2.6 Procedimiento de formulación y ejecución de proyectos.

➢**Objetivo:** el objetivo de este procedimiento es establecer los pasos que constituyen la ejecución de proyectos.

➢**Alcance:** incluye los pasos de visita previa al cliente, negociación, seguimiento, entrega formal, informe técnico y facturación.

➢**Responsables:** Fernando Muñoz y Julián Orjuela.

7.4.2.7 Procedimiento de servicio técnico y mantenimiento de equipos.

➢**Objetivo:** el procedimiento define los pasos que debe seguir el personal contratista en cuanto al soporte técnico y mantenimiento de equipos.

➢**Alcance:** "abarca los pasos desde la solicitud de servicio por parte del cliente e incluye la visita de campo, reporte técnico, recomendaciones y generación de facturas"[16].

➢**Responsables:** Fernando Muñoz y Edwin Gómez.

[16] PORTAL ISO 9001. Procedimientos documentados. [en línea]. Bogotá: ISO, 2014 [fecha de consulta 14 de octubre de 2017]. Disponible en: http://iso9001calidad.com/introduccion-procedimientos-147.html

8. INVENTARIO Y CLASIFICACIÓN DE ACTIVOS

La identificación del inventario de activos permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

De acuerdo con los lineamientos establecidos en la norma ISO 27001:2013, los activos deben ser identificados y se debe definir las responsabilidades de protección apropiadas, lo cual implica valorarlos de acuerdo con su disponibilidad, confidencialidad e integridad. El inventario y clasificación de los activos es la base para la gestión de riesgos de seguridad de la información y para determinar los niveles de protección requeridos.

8.1 IDENTIFICACIÓN DE LOS ACTIVOS

Para la identificación y clasificación de los activos de información, se requiere la participación del gerente general, el cual cuenta con toda la información detallada de cada uno de los activos. En este proceso de Identificación pueden participar personal de la empresa como directos y contratistas.

Los siguientes son los tipos de activos de información que se deben tener en cuenta en el proceso de valoración de activos del proceso.

- Información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

- Software: el software que se utiliza para la gestión de la información (sistema operativo, aplicativos, base de datos, ofimática-documentos electrónicos), software de aplicaciones, etc.

- Tecnología: es todo el hardware donde se maneje la información y las comunicaciones.

- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos – pen drives, discos externos, etc.-), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

Los activos identificados que hacen parte del proceso de levantamiento de información para la empresa SISELCOM S.A.S., se describen a continuación, en el que se visualiza la clasificación de cada uno de ellos.

8.1.1 Inventario de activos. De acuerdo con la norma ISO 27001, en la cual establece la importancia de generar un inventario de activos de equipos físicos, activos de software, activos de tecnología y lógicos, considerando que los activos son de alto valor para la empresa, se tiene que incluir toda la información necesaria para mantenerlos operativos e incluso poder recuperarse ante un desastre. Para facilitar el manejo y mantenimiento del inventario los activos se identifican los siguientes campos en el Cuadro 19 que permiten una mejor administración y gestión de los activos:

- Código: Un código para ordenar y localizar los activos.

- Nombre de Activo: Nombre del activo.

- Tipo de Activo: Catalogación del activo.

- Ubicación: Describe la ubicación tanto física como electrónica del activo de información.

Cuadro 19. Clasificación de activos SISELCOM S.A.S.

Ítem	Código	Nombre Activo	Tipo de Activo	Ubicación
1	ACTF001	Aire Acondicionado Central Viking 60.000 BTU, SEER 10	Activo Físico	ASIC
2	ACTF002	Aire Acondicionado Central Viking 60.000 BTU, SEER 10	Activo Físico	ASIC
3	BAT125	Baterías de soporte 12V 5AH	Activo Físico	Laboratorio
4	BAT127	Baterías de soporte 12V 7AH	Activo Físico	Laboratorio
5	CEL1	Computador escritorio marca Lenovo	Tecnología	Oficina
6	CLC	Celular comercial	Tecnología	Personal
7	CLJ	Celular principal	Tecnología	Personal
8	CPL1	Computador portátil marca Lenovo	Tecnología	Oficina
9	CPL2	Computador portátil marca Lenovo	Tecnología	Oficina
10	CPL3	Computador portátil marca Lenovo	Tecnología	Oficina
11	ESAO	Escritorio asistente oficina	Activo Físico	Oficina
12	ESCO	Escritorio comercial oficina	Activo Físico	Oficina
13	ESL001	Escalera 3.6m 12P	Activo Físico	Laboratorio
14	ESPO	Escritorio principal oficina	Activo Físico	Oficina
15	IO01	Impresora marca Epson	Tecnología	Oficina
16	MNS	Medidor de nivel de sonido	Activo Físico	Laboratorio
17	MRQ	Marquilladora Brady	Activo Físico	Laboratorio
18	PAP	Pinza amperimetrica principal	Activo Físico	Laboratorio
19	PAT	Pinza amperimetrica técnicos	Activo Físico	Laboratorio
20	PCH	Ponchadora	Activo Físico	Laboratorio
21	PD	Probador digital	Activo Físico	Laboratorio
22	PH	Paquete herramienta	Activo Físico	Laboratorio
23	PT001	Planta telefónica Panasonic MAIN UNIT 3 CO, 8 EXT	Tecnología	Almacén
24	SIAO	Silla asistente oficina	Activo Físico	Oficina
25	SIPO	Silla principal oficina	Activo Físico	Oficina
26	TD	Termómetro digital	Activo Físico	Laboratorio

Cuadro 19. (Continuación)

Ítem	Código	Nombre Activo	Tipo de Activo	Ubicación
27	TF	Teléfono fijo	Activo Físico	Oficina
28	VH001	Camioneta Chevrolet Captiva Sport Placa MJW338 Modelo 2012, Color blanco, Cilindraje 2.3, servicio particular.	Activo Físico	Personal
29	AIR012	Aire acondicionado LP1214	Activo Físico	Almacén
30	PE009	Planta eléctrica 6500WT	Activo Físico	Almacén
31	UPS049	UPS soporte online marca Liebert 3 KVA S/N: 8315R1013AF091	Activo Físico	Insepet
32	UPS050	UPS soporte online marca Tripplite 3KVA S/N: 9343ALCPS518500019	Activo Físico	Avisor Technologies
33	UPS051	UPS soporte online marca Soltec 6 KVA S/N: UPS051	Activo Físico	Longport
34	UPS052	UPS soporte online marca Liebert 6Kva S/N: 10208R1023BW571	Activo Físico	Longport
35	UPS053	UPS soporte online marca APC 6Kva S/N: QS1402171870	Activo Físico	Almacén
36	UPS054	UPS soporte online marca Tripplite 10Kva S/N: 2334ALCAC811100017	Activo Físico	SIIGO
37	UPS055	UPS soporte online mrca Liebert 10KVA S/N: 0523401016BWFT2	Activo Físico	SIIGO
38	UPS056	UPS soporte online marca Powercom 12KVA S/N: BQ025A0012	Activo Físico	REDCOM
39	UPS057	UPS soporte online marca Tripplite 3KVA S/N: 9343ALCPS518500082	Activo Físico	Avisor Technologies
40	UPS058	UPS soporte online marca Liebert 3KVA	Activo Físico	Almacén
41	UPS059	UPS soporte online marca Tripplite 3KVA	Activo Físico	Almacén
42	UPS060	UPS soporte marca Liebert 6KVA S/N: 09339R2016AF093	Activo Físico	SAT RET
43	UPS061	UPS soporte online marca Tripplite 3KVA	Activo Físico	JV Parking
44	LIC-MIC1	Licencias sistema operativo y Windows-office	Software	Oficina
45	LIC-MIC2	Licencias sistema operativo y Windows-office	Software	Oficina
46	LIC-MIC3	Licencias sistema operativo y Windows-office	Software	Oficina
47	LIC-MIC4	Licencias sistema operativo y Windows-office	Software	Oficina
48	LIC-CON1	Licencia Word office contable	Software	Oficina
49	LIC-CON2	Licencia Word office contable	Software	Oficina
50	BAS	Base de datos clientes y proveedores	Información	Oficina

Fuente. Los Autores

8.2 VALORACIÓN DE LOS ACTIVOS

En el proceso de valoración de activos, se deben tener en cuenta todos los tipos de activos (activos físicos, activos de software y activos lógicos). Una vez identificados los activos, el siguiente paso a realizar es valorarlos, estimando el valor que tienen para la organización y cuál es su importancia para la misma. Para

calcular este valor, se considera cual puede ser el daño o la afectación que puede suceder a un activo cuando se vea afectado en su disponibilidad, integridad y confidencialidad.
La valoración de los activos permite determinar los activos que son importantes para SISELCOM S.A.S., con los cuales se realizara el posterior análisis de riesgos. Se debe valorar los activos de acuerdo con los atributos de confidencialidad, integridad y disponibilidad. Para realizar dicha valorización, se utiliza una escala cualitativa.

- 1 Bajo: brindándole un código de color verde.
- 2 Medio: brindándole un código de color azul.
- 3 Alto: brindándole un código de color Rojo.

Los activos se identificaron de acuerdo con su tipo, ya sea primario o secundario tal como lo menciona el Anexo B de la norma ISO 27005 en el Cuadro 20. Los mismos fueron valorados de acuerdo con la triada de la seguridad de la información y al impacto que puede llegar a tener para la organización la afectación de cada uno de los mismos.

Cuadro 20. Zonas de valoración de activos

Atributo	Valor	Criterio	Descripción
Disponibilidad	3	Alto	La no disponibilidad del activo impacta negativamente la prestación del servicio. El activo debe estar siempre disponible.
	2	Medio	El activo requiere que esté disponible al menos el 50% del tiempo.
	1	Bajo	Debe estar disponible al menos el 12% del tiempo.
Integridad	3	Alto	La pérdida de funcionalidad del activo impacta negativamente la prestación del servicio.
	2	Medio	Se afecta la Integridad del activo, y la perdida de operatividad afecta parcialmente el servicio.
	1	Bajo	Se afecta la Integridad del activo, y la perdida de operatividad no afecta el servicio.
Confidencialidad	3	Alto	Se hace uso inadecuado del activo al cual se tiene acceso y los daños son muy altos, impacta negativamente la prestación del servicio.
	2	Medio	Se hace uso inadecuado del activo al cual se tiene acceso y los daños son moderables, y la perdida de operatividad afecta parcialmente el servicio.
	1	Bajo	Se hace uso inadecuado del activo al cual se tiene acceso y los daños son muy bajos, el incidente no trasciende en la Organización.

Fuente. Los Autores

Al definir los posibles valores de los diferentes niveles de criticidad, el proceso de valoración de activos de información va ser más simple. La valoración de activos se muestra en el Cuadro 21.

8.2.1 Valoración de activos

Cuadro 21. Valoración de activos

Ítem	Código	Nombre Activo	Tipo de Activo	Ubicación	Disponibilidad	Integridad	Confidencialidad	Nivel
1	ACTF001	Aire Acondicionado Central Viking 60.000 BTU, SEER 10	Equipo Físico	ASIC	Alto	Alto	Alto	Alto
2	ACTF002	Aire Acondicionado Central Viking 60.000 BTU, SEER 10	Equipo Físico	ASIC	Alto	Alto	Alto	Alto
3	BAT125	Baterías de soporte 12V 5AH	Equipo Físico	Laboratorio	Bajo	Medio	Bajo	Bajo
4	BAT127	Baterías de soporte 12V 7AH	Equipo Físico	Laboratorio	Bajo	Medio	Bajo	Bajo
5	CEL1	Computador escritorio marca Lenovo	Tecnología	Oficina	Bajo	Bajo	Bajo	Bajo
6	CLC	Celular comercial	Tecnología	Personal	Medio	Medio	Medio	Medio
7	CLJ	Celular principal	Tecnología	Personal	Medio	Medio	Medio	Medio
8	CPL1	Computador portátil marca Lenovo	Tecnología	Oficina	Bajo	Bajo	Bajo	Bajo
9	CPL2	Computador portátil marca Lenovo	Tecnología	Oficina	Bajo	Bajo	Bajo	Bajo
10	CPL3	Computador portátil marca Lenovo	Tecnología	Oficina	Bajo	Bajo	Bajo	Bajo
11	ESAO	Escritorio asistente oficina	Equipo Físico	Oficina	Bajo	Bajo	Bajo	Bajo
12	ESCO	Escritorio comercial oficina	Equipo Físico	Oficina	Bajo	Bajo	Bajo	Bajo
13	ESL001	Escalera 3.6m 12P	Equipo Físico	Laboratorio	Bajo	Bajo	Bajo	Bajo
14	ESPO	Escritorio principal oficina	Equipo Físico	Oficina	Bajo	Bajo	Bajo	Bajo
15	IO01	Impresora marca Epson	Tecnología	Oficina	Medio	Medio	Medio	Medio
16	MNS	Medidor de nivel de sonido	Equipo Físico	Laboratorio	Bajo	Bajo	Bajo	Bajo

Cuadro 21. (Continuación)

Ítem	Código	Nombre Activo	Tipo de Activo	Ubicación	Disponibilidad	Integridad	Confidencialidad	Nivel
17	MRQ	Marquilladora Brady	Equipo Físico	Laboratorio	Bajo	Bajo	Bajo	Bajo
18	PAP	Pinza amperimetrica principal	Equipo Físico	Laboratorio	Bajo	Bajo	Bajo	Bajo
19	PAT	Pinza amperimetrica técnicos	Equipo Físico	Laboratorio	Bajo	Bajo	Bajo	Bajo
20	PCH	Ponchadora	Equipo Físico	Laboratorio	Bajo	Bajo	Bajo	Bajo
21	PD	Probador digital	Equipo Físico	Laboratorio	Bajo	Bajo	Bajo	Bajo
22	PH	Paquete herramienta	Equipo Físico	Laboratorio	Bajo	Bajo	Bajo	Bajo
23	PT001	Planta telefónica Panasonic MAIN UNIT 3 CO, 8 EXT	Tecnología	Almacén	Medio	Medio	Medio	Medio
24	SIAO	Silla asistente oficina	Equipo Físico	Oficina	Bajo	Bajo	Bajo	Bajo
25	SIPO	Silla principal oficina	Equipo Físico	Oficina	Bajo	Bajo	Bajo	Bajo
26	TD	Termómetro digital	Equipo Físico	Laboratorio	Bajo	Bajo	Bajo	Bajo
27	TF	Teléfono fijo	Equipo Físico	Oficina	Medio	Medio	Medio	Medio
28	VH001	Camioneta Chevrolet Captiva Sport Placa MJW338 Modelo 2012, Color blanco, Cilindraje 2.3, servicio particular.	Equipo Físico	Personal	Alto	Alto	Alto	Alto
29	AIR012	Aire acondicionado LP1214	Equipo Físico	Almacén	Bajo	Bajo	Bajo	Bajo
30	PE009	Planta eléctrica 6500WT	Equipo Físico	Almacén	Bajo	Bajo	Bajo	Bajo

Cuadro 21. (Continuación)

Ítem	Código	Nombre Activo	Tipo de Activo	Ubicación	Disponibilidad	Integridad	Confidencialidad	Nivel
31	UPS049	UPS soporte online marca Liebert 3 KVA S/N: 8315R1013AF091	Equipo Físico	Insepet	Alto	Alto	Alto	Alto
32	UPS050	UPS supporter online marca Tripplite 3KVA S/N: 9343ALCPS518500019	Equipo Físico	Avisor Technologies	Alto	Alto	Alto	Alto
33	UPS051	UPS soporte online marca Soltec 6 KVA S/N: UPS051	Equipo Físico	Longport	Alto	Alto	Alto	Alto
34	UPS052	UPS soporte online marca Liebert 6Kva S/N: 10208R1023BW571	Equipo Físico	Longport	Alto	Alto	Alto	Alto
35	UPS053	UPS soporte online marca APC 6Kva S/N: QS1402171870	Equipo Físico	Almacén	Bajo	Medio	Medio	Medio
36	UPS054	UPS soporte online marca Tripplite 10Kva S/N: 2334ALCAC811100017	Equipo Físico	SIIGO	Alto	Alto	Alto	Alto
37	UPS055	UPS soporte online mrca Liebert 10KVA S/N: 0523401016BWFT2	Equipo Físico	SIIGO	Alto	Alto	Alto	Alto
38	UPS056	UPS soporte online marca Powercom 12KVA S/N: BQ025A0012	Equipo Físico	REDCOM	Alto	Alto	Alto	Alto
39	UPS057	UPS soporte online marca Tripplite 3KVA S/N: 9343ALCPS518500082	Equipo Físico	Avisor Technologies	Alto	Alto	Alto	Alto
40	UPS058	UPS soporte online marca Liebert 3KVA	Equipo Físico	Almacén	Bajo	Medio	Medio	Medio
41	UPS059	UPS soporte online marca Tripplite 3KVA	Equipo Físico	Almacén	Bajo	Bajo	Bajo	Bajo
42	UPS060	UPS soporte marca Liebert 6KVA S/N: 09339R2016AF093	Equipo Físico	SAT RET	Alto	Alto	Alto	Alto

Cuadro 21. (Continuación)

Ítem	Código	Nombre Activo	Tipo de Activo	Ubicación	Disponibilidad	Integridad	Confidencialidad	Nivel
43	UPS061	UPS soporte online marca Tripplite 3KVA UPS061	Equipo Físico	JV Parking	Alto	Alto	Alto	Alto
44	LIC-MIC1	Licencias sistema operativo y Windows- office	Software	Oficina	Bajo	Bajo	Bajo	Bajo
45	LIC-MIC2	Licencias sistema operativo y Windows- office	Software	Oficina	Bajo	Bajo	Bajo	Bajo
46	LIC-MIC3	Licencias sistema operativo y Windows- office	Software	Oficina	Bajo	Bajo	Bajo	Bajo
47	LIC-MIC4	Licencias sistema operativo y Windows- office	Software	Oficina	Bajo	Bajo	Bajo	Bajo
48	LIC-CON1	Licencia Word office contable	Software	Oficina	Medio	Medio	Medio	Medio
49	LIC-CON2	Licencia Word office contable	Software	Oficina	Medio	Medio	Medio	Medio
50	BAS	Base de datos clientes y proveedores	Lógico	Oficina	Alto	Alto	Alto	Alto

Fuente. Los Autores

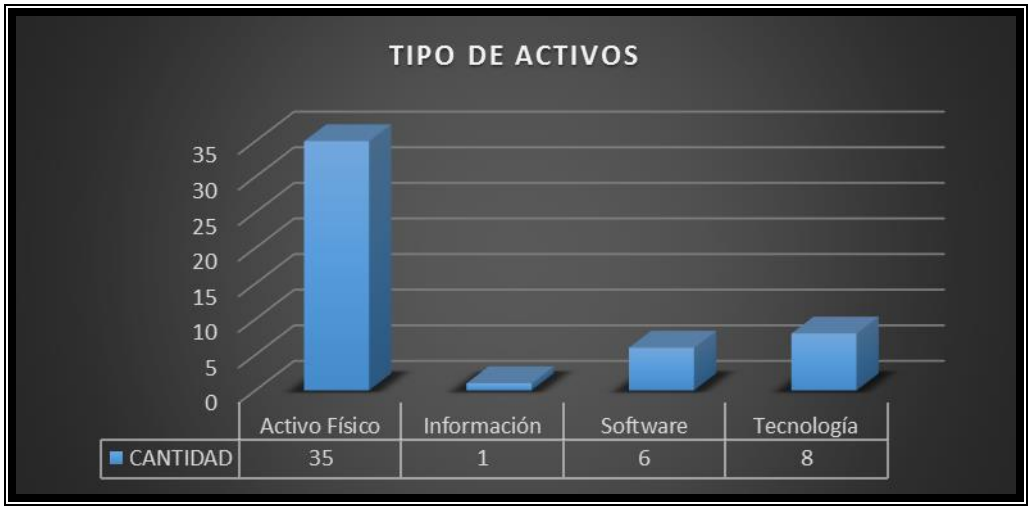
Luego de realizar la valoración de los activos y teniendo en cuenta la valoración de la disponibilidad, la confidencialidad e integridad, se encontraron los siguientes porcentajes en la Figura 35 Porcentaje de valoración de activos.

Figura 35. Porcentaje valoración de activos

Fuente. Los Autores

En la valoración de activos se puede evidenciar en la Figura 36 que 14 activos son clasificados como altos en un 28%, lo cual indica que son están valorados e impacta negativamente la prestación del servicio e impacta negativamente a la Organización.

Figura 36. Tipos de activos



Fuente. Los Autores

De esta clasificación también se puede conocer la distribución por tipos de activo, lo que permitirá enfocar el análisis de riesgos. La anterior figura, muestra los activos de información agrupados por el tipo de activo, en donde 35 de ellos corresponden a Activos físicos que son de gran importancia para la empresa.

9. IDENTIFICACIÓN Y CLASIFICACIÓN DE RIESGOS

Como parte del estudio se llevó a cabo una visita de campo, que permitió identificar los daños y el impacto de incidentes de seguridad. El análisis de riesgo se requiere para establecer que activos están bajo riesgo, logrando con esto que la alta gerencia tome decisiones y definiendo cuales serán aceptados y que mecanismos serán aplicados en búsqueda de mitigar eficientemente estos riesgos.

De acuerdo con la norma ISO/IEC 27001:2013, la organización debe definir y aplicar un proceso de evaluación de riesgos de la seguridad de la información.

9.1 AMENAZAS Y VULNERABILIDADES

Los activos diariamente están expuestos a muchos tipos de amenazas que pueden afectar a los activos provocando pérdidas en la empresa.

Para este proyecto, por cada activo de información se identificarán las amenazas y vulnerabilidades a los cuales pueden estar expuestos, lo que dará como resultado las causas de riesgo presentes en los activos de información del proceso. En consecuencia, se realiza el cuadro de posibles amenazas y vulnerabilidades a las cuales puedan estar expuestos los activos del proceso dentro de la empresa SISELCOM S.A.S.

9.1.1 Clasificación de amenazas. Los activos están sometidos a muchos tipos de amenazas. Una amenaza tiene potencial de causar daño a un activo y por lo tanto a una organización. Existen diferentes fuentes de amenazas que se listan en el Cuadro 22, tomando como referencia la norma ISO 27005 Anexo C:

Cuadro 22. Fuente de las amenazas

Origen	Identificación	Descripción
Accidental	A	Daño accidental a los activos de información.
Deliberado	D	Daño voluntario o intencionado a los activos de información.
Ambiental	E	Daño de origen natural y no por acciones humanas.

Fuente. Los Autores

Una vez identificadas las fuentes de amenazas, en el Cuadro 23 se indican las amenazas más comunes en la empresa:

Cuadro 23. Identificación de amenazas

Tipo	Amenaza	Origen
Daño físico	Fuego.	A, D, E
	Daño por agua.	A, D, E
	Destrucción del equipo.	A, D, E
	Polvo, corrosión.	A, D, E
Eventos naturales	Fenómenos climáticos.	E
	Fenómenos sísmicos.	E
	Inundación.	E
Compromiso de la información	Hurto de medios o documentos.	D
	Hurto de equipo.	D
	Divulgación.	A,D
Fallas técnicas	Falla del equipo.	A
	Mal funcionamiento del equipo.	A
	Incumplimiento en el mantenimiento.	A,D
Acciones no autorizadas	Uso no autorizado del equipo.	D
	Corrupción de los datos.	D
Compromiso de las funciones	Procesamiento ilegal de los datos.	D
	Abuso de derechos.	A,D
Fuente. Los Autores		

9.1.2 Identificación de vulnerabilidades. Las vulnerabilidades son debilidades de los activos de información que pueden ser aprovechados por cualquier persona. Luego de determinar las amenazas más comunes, en el Cuadro 24 se muestran las vulnerabilidades identificadas asociadas a la empresa, tomando como referencia la norma ISO 27005 Anexo D:

Cuadro 24. Vulnerabilidades

Tipo de activo	Vulnerabilidad
FISICOS	Mantenimiento insuficiente.
	Ubicación en un área susceptible de inundación.
	Susceptibilidad a la humedad, el polvo y la suciedad.
	Almacenamiento sin protección.
	Falta de protección física.
	Susceptibilidad a las variaciones de temperatura.
SOFTWARE	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.
	Descarga y uso no controlados de software.
INFORMACION	Divulgación no autorizada sobre la información de los clientes, generando pérdida de confianza en la compañía y acciones legales contra la misma.
	Eliminación accidental o intencional de archivos que puede producir afectación en el desarrollo operacional de la compañía.
	Conservar contraseñas de inicio de sesión en plataformas en las que se almacena información sensible.
	Pérdida de confidencialidad sobre información contractual de los clientes.

Cuadro 24. (Continuación)

Tipo de activo	Vulnerabilidad
TECNOLOGIA	Ausencia de políticas sobre limpieza de escritorio.
	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.
	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario.
	Gestión deficiente de las contraseñas.
	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.
	Falta de protección física de las puertas y ventanas.
	Utilización inapropiada de dispositivos.

Fuente. Los Autores

9.2 NIVEL DE RIESGO

Dentro del proceso de análisis y mitigación, es necesario realizar una matriz de riesgos en la cual se definen las acciones mitigatorias y la reducción de las vulnerabilidades encontradas. El proceso de valoración de riesgos ayuda a estimar la magnitud de las amenazas que están presentes en la empresa y que a través de los planes de tratamiento se pueden tomar medidas preventivas o correctivas ante eventos que puedan causar daño.

Inicialmente se establecen las zonas de riesgo para el análisis.

Cuadro 25. Zonas de riesgo

Nivel de riesgo	Descripción
Alto	Corresponde al nivel de riesgo más alto y el cual contempla que los riesgos encontrados deben ser controlados de manera inmediata, capaz de prevenir, reducir, transferir o compartir el riesgo.
Riesgoso	Corresponde al nivel de riesgo que se encuentra en el límite de afectación por los que los riesgos deben ser tratados con un fin, evitarlos.
Moderado	Corresponde a un nivel permisible, de tal manera que se deben monitorear para que se reduzcan eficientemente.
Aceptable	Corresponde a un nivel en el cual se deben monitorear los riesgos para que no pasen a un nivel de criticidad superior.

Fuente. Los Autores

En el Cuadro 25. Zonas de riesgo, se establecen las zonas de calor del mapa de riesgos, con esto se valora cada activo de la empresa. En el mapa de calor del Cuadro 26 se toma en cuenta la probabilidad de ocurrencia del evento vs el impacto de ocurrencia del evento y la criticidad del riesgo. Con la multiplicación de

estas dos variables se obtiene el resultado para cada zona de riesgo. Cada zona de riesgo tiene un tratamiento especial para los riesgos encontrados.

Cuadro 26. Mapa de calor

Probabilidad	Valor	Zonas de riesgo		
3	Alta	[30] Moderado	[60] Riesgoso	[90] Alto
2	Media	[20] Aceptable	[40] Moderado	[60] Riesgoso
1	Baja	[10] Aceptable	[20] Aceptable	[30] Moderado
	IMPACTO	Bajo	Medio	Alto
	VALOR	10	20	30

Fuente. Los Autores

Al ubicar los riesgos en el mapa de riesgos, la empresa puede tomar decisiones respecto a la forma como debe abordarlos. El mapa es el resultado del análisis de riesgos que se hace en la matriz de riesgos.

9.3 MATRIZ DE RIESGOS

Luego de evaluar y definir la probabilidad y el impacto en el negocio que pueda ocasionar la materialización de los riesgos se obtiene el nivel del riesgo para cada activo de información, como se relaciona en el Cuadro 27.

Cuadro 27. Matriz de riesgos

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
ACTF001	Aire Acondicionado Central Viking 60.000 BTU, SEER 10	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
ACTF002	Aire Acondicionado Central Viking 60.000 BTU, SEER 10	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
BAT125	Baterías de soporte 12V 5AH	Equipo Físico	Fuego.	Almacenamiento sin protección.	[3] Alta	[20] Medio	[60] Riesgoso
			Daño por agua.	Ubicación en un área susceptible de inundación.			
			Destrucción del equipo.	Falta de protección física.			
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
			Hurto de equipo.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
BAT127	Baterías de soporte 12V 7AH	Equipo Físico	Fuego.	Almacenamiento sin protección.	[3] Alta	[20] Medio	[60] Riesgoso
			Daño por agua.	Ubicación en un área susceptible de inundación.			
			Destrucción del equipo.	Falta de protección física.			
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
			Hurto de equipo.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
CEL1	Computador escritorio marca Lenovo	Tecnología	Daño por agua.	Ubicación en un área susceptible de inundación.	[3] Alta	[30] Alto	[90] Alto
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física de las puertas y ventanas.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
			Corrupción de los datos.	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.			
			Abuso de derechos.	Ausencia de políticas sobre limpieza de escritorio.			
CLC	Celular comercial	Tecnología	Daño por agua.	Susceptibilidad a la humedad, el polvo y la suciedad.	[3] Alta	[20] Medio	[60] Riesgoso
			Hurto de equipo.	Falta de protección física de las puertas y ventanas.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
			Corrupción de los datos.	Pérdida de confidencialidad sobre información contractual de los clientes.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
CLJ	Celular principal	Tecnología	Daño por agua.	Susceptibilidad a la humedad, el polvo y la suciedad.	[3] Alta	[20] Medio	[60] Riesgoso
			Hurto de equipo.	Falta de protección física de las puertas y ventanas.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
			Corrupción de los datos.	Pérdida de confidencialidad sobre información contractual de los clientes.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
CPL1	Computador portátil marca Lenovo	Tecnología	Daño por agua.	Ubicación en un área susceptible de inundación.	[3] Alta	[30] Alto	[90] Alto
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física de las puertas y ventanas.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
			Corrupción de los datos.	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.			
			Abuso de derechos.	Ausencia de políticas sobre limpieza de escritorio.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
CPL2	Computador portátil marca Lenovo	Tecnología	Daño por agua.	Ubicación en un área susceptible de inundación.	[3] Alta	[30] Alto	[90] Alto
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física de las puertas y ventanas.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
			Corrupción de los datos.	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.			
			Abuso de derechos.	Ausencia de políticas sobre limpieza de escritorio.			
CPL3	Computador portátil marca Lenovo	Tecnología	Daño por agua.	Ubicación en un área susceptible de inundación.	[3] Alta	[30] Alto	[90] Alto
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física de las puertas y ventanas.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Corrupción de los datos.	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.			
			Abuso de derechos.	Ausencia de políticas sobre limpieza de escritorio.			
ESAO	Escritorio asistente oficina	Equipo Físico	Fuego.	Almacenamiento sin protección.	[1] Baja	[10] Bajo	[10] Aceptable
			Daño por agua.	Ubicación en un área susceptible de inundación.			
			Destrucción del equipo.	Falta de protección física.			
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Fenómenos sísmicos.	Falta de protección física.			
			Hurto de equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
ESCO	Escritorio comercial oficina	Equipo Físico	Fuego.	Almacenamiento sin protección.	[1] Baja	[10] Bajo	[10] Aceptable
			Daño por agua.	Ubicación en un área susceptible de inundación.			
			Destrucción del equipo.	Falta de protección física.			
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Fenómenos sísmicos.	Falta de protección física.			
			Hurto de equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
ESL001	Escalera 3.6m 12P	Equipo Físico	Fuego.	Almacenamiento sin protección.	[1] Baja	[10] Bajo	[10] Aceptable
			Daño por agua.	Ubicación en un área susceptible de inundación.			
			Destrucción del equipo.	Falta de protección física.			
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Fenómenos sísmicos.	Falta de protección física.			
			Hurto de equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
ESPO	Escritorio principal oficina	Equipo Físico	Fuego.	Almacenamiento sin protección.	[1] Baja	[10] Bajo	[10] Aceptable
			Daño por agua.	Ubicación en un área susceptible de inundación.			
			Destrucción del equipo.	Falta de protección física.			
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Fenómenos sísmicos.	Falta de protección física.			
			Hurto de equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
IO01	Impresora marca Epson	Tecnología	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[20] Medio	[40] Moderado
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física de las puertas y ventanas.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
			Corrupción de los datos.	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.			
			Abuso de derechos.	Ausencia de políticas sobre limpieza de escritorio.			
MNS	Medidor de nivel de sonido	Equipo Físico	Destrucción del equipo.	Almacenamiento sin protección.	[3] Alta	[10] Bajo	[30] Moderado
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física.			
			Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
MRQ	Marquilladora Brady	Equipo Físico	Destrucción del equipo.	Almacenamiento sin protección.	[3] Alta	[10] Bajo	[30] Moderado
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física.			
			Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
PAP	Pinza amperimetrica principal	Equipo Físico	Destrucción del equipo.	Almacenamiento sin protección.	[3] Alta	[10] Bajo	[30] Moderado
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física.			
			Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
PAT	Pinza amperimetrica técnicos	Equipo Físico	Destrucción del equipo.	Almacenamiento sin protección.	[3] Alta	[10] Bajo	[30] Moderado
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
PCH	Ponchadora	Equipo Físico	Destrucción del equipo.	Almacenamiento sin protección.	[3] Alta	[10] Bajo	[30] Moderado
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física.			
			Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
PD	Probador digital	Equipo Físico	Destrucción del equipo.	Almacenamiento sin protección.	[3] Alta	[10] Bajo	[30] Moderado
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física.			
			Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
PH	Paquete herramienta	Equipo Físico	Destrucción del equipo.	Almacenamiento sin protección.	[3] Alta	[10] Bajo	[30] Moderado
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física.			
			Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
PT001	Planta telefónica Panasonic MAIN UNIT 3 CO, 8 EXT	Tecnología	Daño por agua.	Ubicación en un área susceptible de inundación.	[1] Baja	[30] Alto	[30] Moderado
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física de las puertas y ventanas.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
			Corrupción de los datos.	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.			
			Abuso de derechos.	Ausencia de políticas sobre limpieza de escritorio.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
SIAO	Silla asistente oficina	Equipo Físico	Fuego.	Almacenamiento sin protección.	[1] Baja	[10] Bajo	[10] Aceptable
			Daño por agua.	Ubicación en un área susceptible de inundación.			
			Destrucción del equipo.	Falta de protección física.			
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Fenómenos sísmicos.	Falta de protección física.			
			Hurto de equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
SIPO	Silla principal oficina	Equipo Físico	Fuego.	Almacenamiento sin protección.	[1] Baja	[10] Bajo	[10] Aceptable
			Daño por agua.	Ubicación en un área susceptible de inundación.			
			Destrucción del equipo.	Falta de protección física.			
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Fenómenos sísmicos.	Falta de protección física.			
			Hurto de equipo.	Uso inadecuado o descuidado del control de acceso físico			
TD	Termómetro digital	Equipo Físico	Destrucción del equipo.	Almacenamiento sin protección.	[3] Alta	[10] Bajo	[30] Moderado
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Hurto de equipo.	Falta de protección física.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
TF	Teléfono fijo	Equipo Físico	Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.	[1] Baja	[10] Bajo	[10] Aceptable
			Hurto de equipo.	Falta de protección física de las puertas y ventanas.			
			Falla del equipo.	Utilización inapropiada de dispositivos.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
			Corrupción de los datos.	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.			
			Abuso de derechos.	Ausencia de políticas sobre limpieza de escritorio.			
VH001	Camioneta Chevrolet Captiva Sport Placa MJW338 Modelo 2012, Color blanco ártico,	Equipo Físico	Destrucción del equipo.	Almacenamiento sin protección.	[2] Media	[30] Alto	[60] Riesgoso
			Fenómenos climáticos.	Falta de protección física.			
			Fenómenos sísmicos.	Falta de protección física.			
			Hurto de equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
	Cilindraje 2,384, servicio particular.		Mal funcionamiento del equipo.	Mantenimiento insuficiente.			
AIR012	Aire acondicionado LP1214	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
PE009	Planta eléctrica 6500WT	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS049	UPS soporte online marca Liebert 3 KVA S/N: 8315R1013 AF091	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS050	UPS soporte online marca Tripplite 3KVA S/N: 9343ALCPS 518500019	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS051	UPS soporte online marca Soltec 6 KVA S/N: UPS051	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS052	UPS soporte online marca Liebert 6Kva S/N: 10208R1023 BW571	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS053	UPS soporte online marca APC 6Kva S/N: QS1402171870	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS054	UPS soporte online marca Tripplite 10Kva S/N: 2334ALCAC811100017	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS055	UPS soporte online mrca Liebert 10KVA S/N: 0523401016 BWFT2	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS056	UPS soporte online marca Powercom 12KVA S/N: BQ025A001 2	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS057	UPS soporte online marca Tripplite 3KVA S/N: 9343ALCPS 518500082	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS058	UPS soporte online marca Liebert 3KVA	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS059	UPS soporte online marca Tripplite 3KVA	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS060	UPS soporte marca Liebert 6KVA S/N: 09339R2016 AF093	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
UPS061	UPS soporte online marca Tripplite 3KVA UPS061	Equipo Físico	Daño por agua.	Ubicación en un área susceptible de inundación.	[2] Media	[30] Alto	[60] Riesgoso
			Polvo, corrosión.	Susceptibilidad a la humedad, el polvo y la suciedad.			
			Destrucción del equipo.	Falta de protección física.			
			Hurto de equipo.	Almacenamiento sin protección.			
			Falla del equipo.	Mantenimiento insuficiente.			
			Fenómenos sísmicos.	Falta de protección física.			
			Uso no autorizado del equipo.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.			
LIC-MIC1	Licencias sistema operativo y Windows-office	Software	Mal funcionamiento del equipo.	Utilización inapropiada de dispositivos.	[1] Baja	[30] Alto	[30] Moderado
			Procesamiento ilegal de los datos.	Descarga y uso no controlados de software.			
			Abuso de derechos.	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
LIC-MIC2	Licencias sistema operativo y Windows-office	Software	Mal funcionamiento del equipo.	Utilización inapropiada de dispositivos.	[1] Baja	[30] Alto	[30] Moderado
			Procesamiento ilegal de los datos.	Descarga y uso no controlados de software.			
			Abuso de derechos.	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.			
LIC-MIC3	Licencias sistema operativo y Windows-office	Software	Mal funcionamiento del equipo.	Utilización inapropiada de dispositivos.	[1] Baja	[30] Alto	[30] Moderado
			Procesamiento ilegal de los datos.	Descarga y uso no controlados de software.			
			Abuso de derechos.	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.			
LIC-MIC4	Licencias sistema operativo y Windows-office	Software	Mal funcionamiento del equipo.	Utilización inapropiada de dispositivos.	[1] Baja	[30] Alto	[30] Moderado
			Procesamiento ilegal de los datos.	Descarga y uso no controlados de software.			
			Abuso de derechos.	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.			

Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
LIC-CON1	Licencia Word office contable	Software	Mal funcionamiento del equipo.	Utilización inapropiada de dispositivos.	[1] Baja	[30] Alto	[30] Moderado
			Procesamiento ilegal de los datos.	Descarga y uso no controlados de software.			
			Abuso de derechos.	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.			
LIC-CON2	Licencia Word office contable	Software	Mal funcionamiento del equipo.	Utilización inapropiada de dispositivos.	[1] Baja	[30] Alto	[30] Moderado
			Procesamiento ilegal de los datos.	Descarga y uso no controlados de software.			
			Abuso de derechos.	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.			
BAS	Base de datos clientes y proveedores	Logico	Hurto de medios o documentos.	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.	[3] Alta	[30] Alto	[90] Alto
			Divulgación.	Divulgación no autorizada sobre la información de los clientes, generando pérdida de confianza en la compañía y acciones legales contra la misma.			

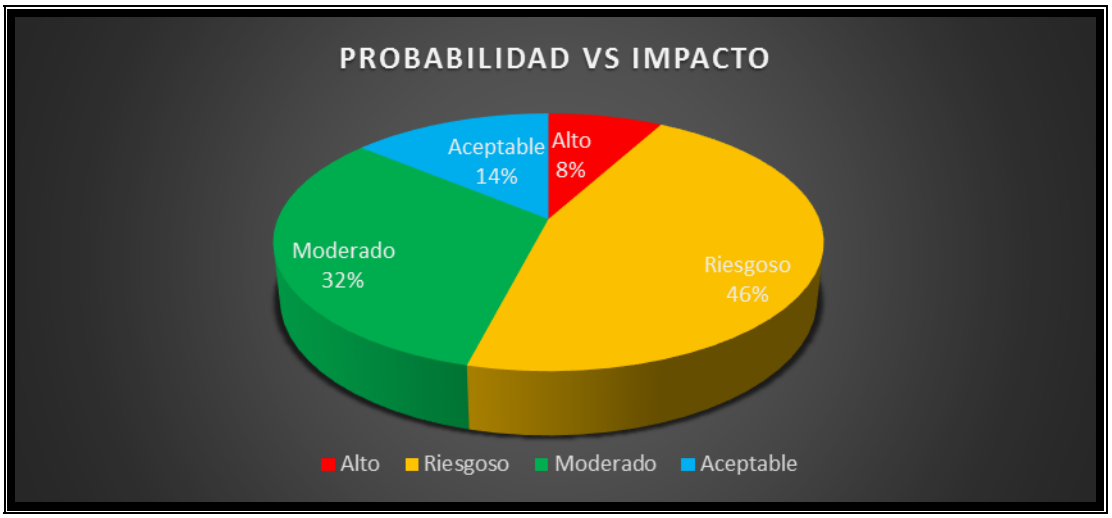
Cuadro 27. (Continuación)

Identificacion del riesgo					Analisis de riesgo		
Código	**Nombre Activo**	**Tipo de Activo**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
			Corrupción de los datos.	Eliminación accidental o intencional de archivos que puede producir afectación en el desarrollo operacional de la compañía.			
			Procesamiento ilegal de los datos.	Pérdida de confidencialidad sobre información contractual de los clientes.			
			Abuso de derechos.	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario.			

Fuente. Los Autores

Se realizó el proceso de analisis a 50 activos de la empresa los cuales, de acuerdo a su nivel de riesgo, en la Figura 37 se observa que se distribuyen de la siguiente forma: 7 (14%) clasificados como riesgo Aceptable, 16 (32%) clasificados como riesgo Moderado, 23 (46%) clasificados como riesgo Riesgoso y 4 (8%) clasificados como riesgo Alto.

Figura 37. Probabilidad vs impacto



Fuente. Los Autores

En el Cuadro 28 se ubican los activos de acuerdo con su nivel de riesgo, así la empresa puede tener una visión más clara de cómo se encuentran sus activos y las acciones a seguir:

Cuadro 28. Activos y nivel de riesgo

Probabilidad	Zonas de riesgo		
Alta	MNS, MRQ, PAP, PAT, PCH, PD, PH, TD	BAT125, BAT127, CLC, CLJ	CPL1, CPL2, CPL3, BAS
Media		IO01	ACTF001, ACTF002, CEL1, VH001, AIR012, PE009, UPS049, UPS050, UPS051, UPS052, UPS053, UPS054, UPS055, UPS056, UPS057, UPS058, UPS059, UPS060, UPS061
Baja	ESAO, ESCO, ESL001, ESPO, SIAO, SIPO, TF		PT001, LIC-MIC1, LIC-MIC2, LIC-MIC3, LIC-MIC4, LIC-CON1, LIC-CON2
IMPACTO	Bajo	Medio	Alto

Fuente. Los Autores

Lo que se puede concluir en este análisis es que en este momento los activos que se encuentran en mayor riesgo son los equipos de cómputo y las bases de datos por lo que se deben tomar acciones inmediatas para tratar estos riesgos y reducir sus vulnerabilidades. En la zona Riesgoso vemos que se encuentran la mayoría de equipos que la empresa tiene almacenados o en alquiler y que son el núcleo del negocio, si se ven afectados pueden representar un costo muy alto para la empresa además de la perdida reputacional por esta razón se recomienda realizar un tratamiento inmediato para mitigar su riesgo.

10. PLAN DE MITIGACIÓN Y SELECCIÓN DE CONTROLES

Al realizar el análisis de riesgo se encontraron diecinueve (19) controles correspondientes al Anexo A de la norma ISO 27001:2013 que corresponden a un riesgo alto para la empresa, por lo que se realizara un análisis puntual y una posible contramedida para estos riesgos. Estos riesgos se organizaron de acuerdo con el numeral dado en la norma por lo que se agruparon por ítems lo que genero un total de 10 hallazgos.

10.1 HALLAZGO 01 POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN

➢**Numeral:** A. 5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN.

➢**Subitem:**

✓A.5.1. Orientación de la dirección para la gestión de la seguridad de la información.

✓A.5.1.1. Políticas para la seguridad de la información.

✓A.5.1.2. Revisión de las políticas para la seguridad de la información.

➢**Criterio:** verificar la existencia de políticas de seguridad que deben ser aprobadas por la gerencia e informadas a todo el personal.

➢**Posibles efectos:**

✓Falta de conocimiento acerca de los riesgos que se tienen en cuanto a la seguridad de la información.

✓Incumplimiento a los parámetros establecidos internos y externos que el sistema proporcional.

✓Falta de control del sistema de información.

➢**Recomendaciones:** se deben definir un conjunto de políticas para la seguridad aprobadas por la gerencia y comunicadas a los empleados, estas políticas se deben revisar a intervalos planificados para validar su cumplimiento.

➢**Posibles costos:** en el desarrollo del presente proyecto se desarrolló una política de seguridad aprobada por la dirección en cuanto a la solución es necesario publicarla a los empleados lo que se realizaría por medio de una socialización o capacitación que no incurría en un costo alto para la organización.

10.2 HALLAZGO 02 SEGURIDAD DE LOS RECURSOS HUMANOS

➢**Numeral:** A. 7. SEGURIDAD DE LOS RECURSOS HUMANOS.

➢**Subitem:**

✓A.7.1. Antes de asumir el empleo.
✓A.7.1.1. Selección.

➢**Criterio:** verificar la implementación de una política de seguridad para todo el personal que trabaja en la empresa.

➢**Posibles efectos:**

✓No se realiza proceso de verificación de antecedentes para el personal que labora en la empresa.

✓No se conocen los antecedentes del personal directo o contratistas que laboran en la empresa y estos pueden manejar información sensible de la empresa, lo que genera un riesgo sobre los activos de la empresa.

✓No hay compromiso ni responsabilidad del empleado y del empleador.

➢**Recomendaciones:** establecer un procedimiento para realizar validación de antecedentes en el proceso de contratación, como estudios de seguridad, validación de referencias, estos se deben realizar de acuerdo con el rol que asuma el nuevo empleado en la empresa. Se debe aplicar tanto para contratos directos como para contratistas.

➢**Posibles costos:** se realizaron diferentes cotizaciones y de acuerdo con el estudio se tiene un "costo aproximado de $80.000 por persona"[17].

10.3 HALLAZGO 03 SEGURIDAD DE LOS RECURSOS HUMANOS

➢**Numeral:** A. 7. SEGURIDAD DE LOS RECURSOS HUMANOS.

➢**Subitem:**

✓A.7.3. Terminación y cambio de empleo.
✓A.7.3.1. Terminación o cambio de responsabilidades de empleo.

[17] GYJ SECURITY CONSULTING GROUP. Seguridad en personas. [en línea]. Bogotá: G&J Group, 2017 [fecha de consulta 7 de agosto de 2017]. Disponible en: http://gyjgroup.com/seguridad-personas.html

➢**Criterio:** se deben proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.

➢**Posibles efectos:**

✓No se evidencia de la existencia de un proceso que establezca acciones formales en el caso de violentar algunos de los sistemas de seguridad.

✓No se evidencia la existencia proceso y/o métodos para informar la terminación o cambio de responsabilidad de empleo.

✓Desconocimiento de la ley.

✓No hay compromiso ni responsabilidad del empleado y del empleador.

➢**Recomendaciones:** la empresa debe informar a sus empleados y contratistas que las responsabilidades y deberes de seguridad de la información permanecen validos después de la terminación o cambio de empleo. Se deben documentar todos los acuerdos de confidencialidad con las partes externas, contemplando el inicio y la finalización de la contratación que evite divulgación de información sensible de la empresa.

➢**Posibles costos:** incluir en los contratos tanto de empleados directos como contratistas una cláusula para que cumplan con los procesos de terminación o cambio de labor no implica ningún costo para la empresa y debe estar en el proceso de capacitación a los empleados.

10.4 HALLAZGO 04 GESTIÓN DE ACTIVOS

➢**Numeral:** A.8. GESTIÓN DE ACTIVOS.

➢**Subitem:**

✓A.8.1. Responsabilidad por los activos.
✓A.8.1.4. Devolución de activos.

➢**Criterio:** verificación de la existencia de una política de seguridad en cuanto a la protección de activos, clasificación de la información y para el manejo de medios de soporte.

➢**Posibles efectos:**

✓No se evidencia la existencia de un proceso de devolución de activos por parte de los empleados.

✓Pérdida de control de los activos.
✓Fuga de información.
✓Uso mal intencionado.

➢**Recomendaciones:** se deben establecer procedimientos para la devolución de activos tanto para los empleados, contratistas y partes externas. Se deben establecer formatos donde se lleve un control de trazabilidad de los activos.

➢**Posibles costos:** se deben documentar todos los procedimientos de la empresa y crear formatos no solo para este numeral sino para los procedimientos que necesite la empresa por lo que se recomienda contratar una persona al menos por 3 meses para realizar la documentación de todos los procesos, esto puede acarrear un costo mensual aproximado de $850.000 para un total de $2´550.000 por los 3 meses.

10.5 HALLAZGO 05 CONTROL DE ACCESO

➢**Numeral:** A.9. CONTROL DE ACCESO.

➢**Subitem:**

✓A.9.1. Requisitos del negocio para el control de acceso.
✓A.9.1.1. Política de control de acceso.

➢**Criterio:** verificar si la empresa tiene un procedimiento detallado y documentado que controle el acceso en todas las áreas que requieren del mismo.

➢**Posibles efectos:**

✓No existe política control de acceso.

✓Desconocimiento del personal de una política de control acceso.

✓Ingreso personal no autorizado - manipulación inadecuada de la información y los servicios.

✓Acceso sin control, para el personal que es ajeno a la entidad mala manipulación y divulgación de la información.

➢**Recomendaciones:** se debe establecer una política de control de acceso que sea aprobada por la dirección de acuerdo con las restricciones y requisitos de seguridad que amerite la empresa. Sensibilizar a todos los miembros de la empresa, la responsabilidad que tienen con la información y las consecuencias que trae el mal uso de los sistemas.

➢**Posibles costos:** el diseño de una política de control de acceso no implica ningún costo para la empresa solo se debe comunicar a los empleados por medio de un proceso de capacitación.

10.6 HALLAZGO 06 SEGURIDAD FÍSICA Y DEL ENTORNO

➢**Numeral:** A.11. SEGURIDAD FÍSICA Y DEL ENTORNO.

➢**Subitem:**

✓A.11.1. Áreas seguras.
✓A.11.1.1. Perímetro de seguridad física.
✓A.11.1.4. Protección contra amenazas externas y ambientales.
✓A.11.1.6. Áreas de despacho y carga.
✓A.11.2. Equipos.
✓A.11.2.1. Ubicación y protección de los equipos.
✓A.11.2.5. Retiro de activos.
✓A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones.

➢**Criterio:** verificar que exista un procedimiento para prevenir el acceso físico no autorizado a la empresa y la protección contra amenazas ambientales.

➢**Posibles efectos:**

✓No se evidencia la delimitación de perímetro de seguridad.

✓No se evidencia la existencia de un procedimiento contra las amenazas ambientales.

✓No se evidencia procedimiento para tratar la política de escritorio limpio.

✓Posible robo o pérdida de información- Robo a daño de activos.

✓Posible daño de activos por desastres naturales, los equipos no se encuentran almacenados de manera segura.

✓Falta de control en los activos.

✓Perjuicio para la imagen empresarial.

➢**Recomendaciones:** se recomienda inicialmente incrementar los controles de seguridad al ingreso de la empresa tanto donde se encuentran los equipos como la información importante o sensible de la empresa. También es importante ubicar los equipos o activos de manera adecuada para evitar posibles daños. Es importante documentar todos los procedimientos y crear formatos para el retiro y

la devolución de activos con las listas de chequeo respectivas para garantizar la integridad de los equipos tanto dentro como fuera de la empresa. Establecer la normatividad vigente para la seguridad física y de la información. Generar mecanismos que prevengan la pérdida de información, hurto o la no disponibilidad de la información.

➢**Posibles costos:**

✓Instalación de cámaras en el ingreso a los equipos y al ingreso al área administrativa, consultado a la gerencia de SISELCOM tendría un costo aproximado de $1.000.00 por las dos cámaras.

✓Racks para "la acomodación correcta de los equipos, con un costo promedio de $1.342.000"[18].

✓La documentación y creación de formatos se incluyó en el hallazgo 4, la misma persona puede realizar esta labor.

10.7 HALLAZGO 07 SEGURIDAD DE LAS OPERACIONES

➢**Numeral:** A.12. SEGURIDAD DE LAS OPERACIONES.

➢**Subitem:**

✓A.12.1. Procedimientos operacionales y responsabilidades.
✓A.12.1.1. Procedimiento de operación documentados.

➢**Criterio:** asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

➢**Posibles efectos:**

✓Desconocimiento en cuanto a la forma de seguir los procedimientos.
✓Por la falta de planeamiento metodológico se puede incurrir en fallas constantes.
✓Modificación de operaciones.
✓Mal manejo de la información.

➢**Recomendaciones:** se deben documentar todos los procedimientos y poner a disposición de todos los usuarios que lo necesiten. Se deben establecer normas de seguridad para los servicios de tercerización, que garanticen la responsabilidad con la entidad.

[18] MERCADO LIBRE. Muebles para Oficinas Vitrinas Comerciales. [en línea]. Bogotá: Mercado Libre, 2017 [fecha de consulta 7agosto de 2017]. Disponible en: http://articulo.mercadolibre.com .co/MCO-445587912-shelving-estanteria-stocker-en-metal-y-madera-de-200x18-hct2-_JM

➢**Posibles costos:** la documentación y creación de formatos se incluyó en el hallazgo 4, la misma persona puede realizar esta labor.

10.8 HALLAZGO 08 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

➢**Numeral:** A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

➢**Subitem:**

✓A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.

✓A.16.1.3. Reporte de debilidades de seguridad de la información.

✓A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

✓A.16.1.5. Respuesta a incidentes de seguridad de la información.

➢**Criterio:** asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

➢**Posibles efectos:**

✓No se evidencia procedimientos de gestión de incidentes
✓Desconocimiento de los riesgos e incidentes.
✓Desconocimiento de los eventos de seguridad.
✓Desconocimiento del propio sistema de seguridad y avances del mismo.
✓Pérdida de información valiosa para el tema de los incidentes encontrados.

➢**Recomendaciones:** se deben diseñar procedimientos para la gestión de incidentes y eventos de seguridad que incluyan el reporte de eventos, reportes de debilidades, respuesta a incidentes, recolección de evidencia y lecciones aprendidas.

➢**Posibles costos:** la documentación y creación de formatos se incluyó en el hallazgo 4, la misma persona puede realizar esta labor.

10.9 HALLAZGO 9 CONTINUIDAD DE NEGOCIO

➢**Numeral:** A.17. CONTINUIDAD DE NEGOCIO.

➢**Subitem:**

✓A.17.1. Continuidad de seguridad de la información.
✓A.17.1.1. Planificación de la continuidad de la seguridad de la información.

➢**Criterio:** verificar la existencia de una política de seguridad que asegure la continuidad el negocio.

➢**Posibles efectos:**

✓No se evidencia planificación de la continuidad de la seguridad de la información.

✓No se evidencia que exista una verificación de los controles de la seguridad de la información.

✓Falta de documentación importante para el proceso de seguridad.

✓Des aseguramiento de la información en todos los niveles.

✓Estancamiento de la entidad en la seguridad de la información

➢**Recomendaciones:** se deben establecer y determinar los requisitos para la seguridad de la información y la continuidad del negocio para situaciones adversas como una crisis o desastre. Se deben desarrollar procedimientos de recuperación, retorno, pruebas con el fin de asegurar la restauración de los servicios y sistemas, lo cuales deben ser revisados y actualizados periódicamente.

➢**Posibles costos:** esto lo debe determinar la gerencia y generar la respectiva documentación que no generara ningún costo adicional para la empresa.

10.10 HALLAZGO 10 CUMPLIMIENTO

➢**Numeral:** A.18. CUMPLIMIENTO.

➢**Subitem:**

✓A.18.2. Revisiones de seguridad de la información.
✓A.18.2.2. Cumplimiento con las políticas y normas de seguridad.
✓A.18.2.3. Revisión del cumplimiento técnico.

➢**Criterio:** asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

➢**Posibles efectos:**

✓No se evidencia el cumplimiento y seguimiento de las políticas y normas de seguridad.

✓No se evidencia que se realice una revisión del cumplimiento técnico.

✓Des aseguramiento de la información.

✓Incremento en fallas técnicas.

➢**Recomendaciones:** se deben establecer mecanismos de control que garanticen la seguridad de la protección de los sistemas y las auditorias del sistema. La información que es clasificada como confidencial se debe proteger de acuerdo con el marco legal.

➢**Posibles costos:** la gerencia debe realizar revisiones del cumplimiento de políticas y procedimientos con regularidad, pero esto no acarrea costos adicionales en la empresa.

Cuadro 29. Costos totales

Hallazgo	Posible costo
Estudio de seguridad	$ 80.000,00
Persona encargada de la documentación	$ 2.550.000,00
Cámaras de seguridad	$ 1.000.000,00
Racks para acomodación de equipos	$ 1.342.000,00
Total	**$ 4.972.000,00**

Fuente. Los Autores

En el Cuadro 29 se observa que en realidad, los costos asociados a reducir los riesgos altos en la empresa no son tan altos como se espera por lo que es totalmente viable aplicar las recomendaciones dadas y así proteger la información y los activos de la empresa.

11. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SISELCOM S.A.S., empresa dedicada a la asesoría, construcción y prestación de servicios de ingeniería eléctrica y de comunicaciones en el área de suministros, mantenimientos y alquiler de UPS, redes eléctricas, cableado estructurado, acondicionamiento ambiental y circuito cerrado de televisión, en cumplimiento de la misión, visión, para seguridad y satisfacción de los clientes ha establecido la siguiente política de seguridad de la información.

Esta política de seguridad de la información busca la protección de los recursos y la información, de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del negocio de la empresa.

La presente política aplica a toda la empresa, incluyendo a sus colaboradores, proveedores y demás partes interesadas que intervengan en la operación.

Fernando Muñoz
Gerente General

11.1 OBJETIVOS DE LA POLÍTICA DE SEGURIDAD

- Incrementar el nivel de satisfacción de los clientes internos y externos.

- Incrementar el nivel de competencias del talento humano.

- Mantener la integridad de la información de la empresa, teniendo en cuenta los requisitos de seguridad aplicables y los resultados de la valoración y el tratamiento de los riesgos identificados.

- Asegurar que la información de SISELCOM S.A.S., esté disponible para los usuarios o procesos autorizados en el momento en que así lo requieran.

- Asegurar la continuidad del negocio.

11.2 ALCANCE

El presente documento es aplicable a todos los empleados, consultores, contratistas, colaboradores y personal externo que en algún momento cuente con acceso a los recursos informáticos o información de la empresa.

11.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

11.3.1 Política general. SISELCOM S.A.S. establece, define y revisa sus objetivos encaminados a mejorar la seguridad, entendiéndola como la conservación de la confidencialidad, integridad y disponibilidad, así como la de la infraestructura que la soportan.

La gerencia de SISELCOM S.A.S. se compromete a apoyar y mantener las políticas de seguridad de la información. Para ello la empresa implantará las medidas requeridas para la formación y concientización del personal respecto a la seguridad de la información. Adicionalmente, cuando cualquier funcionario incumpla las políticas de seguridad, la gerencia se reserva el hecho de aplicar las medidas disciplinarias acordes aplicables y dimensionadas al impacto que tengan sobre la empresa.

11.3.1.1 Organización de la seguridad de la información. Cada trabajador de SISELCOM S.A.S. debe tener un rol definido para la seguridad de la información, de tal forma que pueda desempeñar su actividad laboral y cumplir a cabalidad con los requerimientos de la empresa.

A continuación, se definen los roles y responsabilidades que deben ser desempeñados por los colaboradores frente a la seguridad de la información:

11.3.1.2 Alta gerencia. La alta gerencia debe revisar y aprobar la política de seguridad de la información, por lo menos una vez al año, o cuando ocurra algún cambio significativo en la empresa. De igual forma debe:

- Asegurar que los requisitos del SGSI se encuentran integrados en los procesos de información en la organización.

- Garantizar la seguridad de la información personal entregada por los colaboradores durante su proceso de vinculación y trabajo en la compañía.

- Comunicar la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del SGSI.

- Promover la mejora continua.

11.3.1.3 Propietario - responsable de los activos. Las principales responsabilidades de este rol incluyen, pero no se limitan a:

- Revisar y asegurar los privilegios de acceso asociados con los activos de información que es responsable.

➢Determinar los requerimientos de seguridad, criterios de acceso y criterios de copias de respaldo para los activos de información de los que es responsable.

11.3.1.4 Todos los usuarios. Las principales responsabilidades de todos los usuarios incluyen, pero no se limitan a:

➢Proteger la información que SISELCOM S.A.S. le ha suministrado para la ejecución de sus labores.

➢Firmar un acuerdo de confidencialidad y/o no divulgación antes de iniciar formalmente sus labores dentro de la compañía,

➢Reconocer que la propiedad intelectual incluyendo sin limitantes, patentes, derechos de autor, marcas registradas y todos los otros derechos de propiedad intelectual tal como se manifiestan en planes, estrategias, productos, programas de computación, documentación y demás material desarrollado o concebido mientras el colaborador esté desarrollando sus labores o gestión en sitios alternativos de trabajo, son exclusiva propiedad de SISELCOM S.A.S.

➢Mantener la confidencialidad de sus contraseñas.

➢Usar los activos de la compañía y los recursos de información de manera segura y adecuada para desempeñar sus funciones laborales.

11.3.1.5 Terceros. Todo contratista, consultor, proveedor o cliente que tenga acceso a la información de SISIELCOM S.A.S. tiene los mismos deberes que un colaborador o un prestador de servicios frente a la protección de la información que le ha sido suministrada.

11.3.1.6 Lineamientos para Dispositivos Móviles

➢**Objetivo.** Establecer las directrices para el uso y manejo adecuado de dispositivos móviles y equipos de terceros.

➢**Directrices:**

✓La instalación de aplicaciones en los computadores portátiles por parte de los colaboradores está prohibida, todos los requerimientos de instalación deben hacerse a la gerencia, quien será la encargada de realizar el proceso.

✓No se deben instalar aplicaciones de fuentes desconocidas en los dispositivos móviles como celulares o tablets.

11.3.2 Políticas de seguridad para los recursos humanos.

11.3.2.1 Objetivo. Definir los lineamientos que se deben aplicar a la gestión del recurso humano, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información.

➢**Directrices antes de asumir el empleo:**

✓Antes de iniciar sus labores dentro de la compañía, los colaboradores que fueron escogidos durante el proceso de selección deben firmar su contrato de trabajo como aceptación de los términos y condiciones de empleo que van a desempeñar.

✓Los colaboradores deben firmar acuerdos de confidencialidad antes que se les otorgue acceso a las instalaciones de procesamiento y/o acceso a la información de SISELCOM S.A.S. o de terceros.

➢**Directrices durante la ejecución del empleo:**

✓Debe comunicarse al nuevo trabajador, contratista y/o tercero sus responsabilidades y derechos legales.

✓La gerencia debe realizar cada año la verificación de antecedentes judiciales para todos los colaboradores, contratistas y terceros.

✓Todos los colaboradores recibirán la educación y formación necesaria para generar conciencia respecto a la seguridad de la información.

➢**Directrices para la terminación y cambio de empleo:**

✓Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo ya sea que el retiro sea voluntario o no voluntario.

11.3.3 Política de gestión de activos de información.

➢**Objetivo:** establecer las directrices para mantener la protección adecuada de los activos de información.

➢**Directrices:** todo activo que esté contemplado dentro del alcance del SGSI, debe tener designado un responsable.

✓El responsable de los activos o el colaborador que este designé, debe recopilar y mantener permanentemente actualizado un inventario de activos de información. Esta revisión debe realizarse con una periodicidad semestral. De acuerdo al acta de entrega de activos SSC_003 en el anexo C.

✓Los activos que SISELCOM S.A.S pone a disposición de sus colaboradores sólo deben ser utilizados para desempeñar funciones asociadas con su rol.

✓Se debe reportar la pérdida o daño los elementos tecnológicos en el formato SSC_002 relacionado en el anexo A, en el menor tiempo posible al director de área correspondiente y este informará posteriormente al área de tecnología. En caso de pérdida el funcionario asumirá el valor.

11.3.4 Políticas de clasificación de la información.

➢**Objetivo:** asegurar que la información recibe un nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley.

➢**Directrices:**

✓Esta política suministra información a todos los funcionarios para guiar el manejo de la seguridad de la información sensible de la compañía.

✓Antes de divulgar información confidencial de SISELCOM S.A.S o recibir información confidencial de terceras partes, debe firmarse un acuerdo de confidencialidad entre las partes.

11.3.5 Política de control de acceso.

➢**Objetivo:** definir los lineamientos para asegurar el acceso físico o lógico, a la información, aplicaciones y/o plataforma de SISELCOM S.A.S.

➢**Directrices:**

✓Cada funcionario dentro de la compañía deberá contar con privilegios y accesos a los diferentes sistemas de información e información de acuerdo a su rol desempeñado dentro de la compañía.

✓Todos los empleados y/o terceros que así lo requieran, tendrán un nombre de usuario y una contraseña que servirán para identificarlos y permitirles el acceso a los sistemas de SISELCOM S.A.S.

✓Cada trabajador debe proteger el acceso a su estación de trabajo cuando esta no se encuentre en uso, asegurando la misma.

✓Los escritorios deben permanecer limpios y despejados. Esto evita exponer su información a otras personas durante su ausencia, además promueve un mejor ambiente de trabajo.

✓Está prohibido el uso o almacenamiento de material obsceno, pornográfico, música o material con fines terroristas, en los equipos o sistemas de información de la compañía.

✓Todo el software, como paquetes de ofimática, sistemas operativos, aplicaciones, antivirus debe estar controlado obedeciendo al rol del área dentro de la empresa.

11.3.6 Política de seguridad física y del entorno.

➢**Objetivo:** definir los lineamientos que deben seguir los usuarios y responsables para acceder a las instalaciones y activos físicos de información, con el fin de asegurar una adecuada protección de la información en SISELCOM S.A.S.

➢**Directrices:**

✓Los materiales peligrosos o combustibles (materiales inflamables) deben ser almacenados en lugares seguros a una distancia prudencial de las áreas de trabajo.

✓Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.

✓Debe certificarse que toda la información sensible ha sido adecuadamente removida de cualquier componente del sistema informático utilizado para los negocios de la empresa, antes de entregar los componentes a terceros.

✓Debe llevarse un control de la entrada y salida de activos o materiales de la empresa en el Formato SSC_001 relacionado en el anexo B.

11.3.7 Política de seguridad de las operaciones.

➢**Objetivo:** definir los lineamientos que deben seguirse para la constante operatividad de la información de SISELCOM S.A.S.

➢**Directrices:**

✓Cualquier proceso de cambio que afecte los sistemas de información debe planificarse y evaluarse para garantizar que este se lleve a cabo de la forma más eficiente, siguiendo siempre las pautas y procedimientos establecidos que aseguren la disponibilidad, integridad confidencialidad de los activos de información.

✓Debe respaldarse periódicamente toda la información confidencial, sensitiva y/o crítica contenida en los sistemas de computación y las redes de SISELCOM

S.A.S. Los responsables de la información deben definir cuál información y cuáles equipos deben respaldarse, así como la frecuencia y el método de respaldo que se empleará, en concordancia con los lineamientos indicados en la presente política.
✓Deben realizarse pruebas a las copias de respaldo como mínimo una vez al año, para asegurar que pueden ser restaurados completamente durante todo el periodo de conservación.

✓Toda tarea de mitigación de hallazgos y vulnerabilidades debe ser evaluada regularmente para garantizar la efectividad y eficiencia del control.

✓Se deben realizar auditorías internas como mínimo una vez al año al Sistema de Gestión de Seguridad de la Información.

✓Debe realizarse un plan de tratamiento de los hallazgos encontrados en las auditorías internas y/o externas. Este plan debe contemplar como mínimo los tiempos de ejecución, impacto de la actividad, responsables, recursos y fechas de implementación.

✓En los sistemas de comunicación que la empresa ha adoptado utilizar, en especial el correo electrónico, debe usarse únicamente para actividades empresariales, se debe evitar el uso irresponsable como reenviar cadenas de correo, spam, publicidad o lenguaje obsceno que interfiera con la productividad del trabajador y no tenga prioridad sobre otras actividades del negocio.

✓El trabajador debe asegurarse que las actualizaciones automáticas de su equipo estén habilitadas. Al hacer que el sistema operativo este actualizado disminuye la probabilidad de que ocurra un ataque de virus o código malicioso sobre su máquina.

11.3.8 Política contra código malicioso.

➢**Objetivo:** definir los lineamientos con los que se deben prevenir los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información.

➢**Directrices:**

✓Debe establecerse los controles de seguridad adecuados para evitar la instalación en equipos de cómputo, servidores, equipos de red y comunicaciones de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.

✓Debe establecerse los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo solo lo pueda realizar personal debidamente autorizado.

11.3.9 Política uso de contraseñas.

➢**Objetivo:** definir los lineamientos que deben seguir los usuarios y responsables de la información para el correcto uso y tratamiento de contraseñas suministradas por SISELCOM S.A.S.

➢**Directrices:** todas las contraseñas de cuentas que den acceso a recursos y servicios de la compañía deberán seguir las siguientes directrices generales:

✓Todas las contraseñas de sistema como root, cuentas de administración de aplicaciones, cuentas de administración de servidores, cuentas de administración de correo, administración de equipos y acceso a redes inalámbricas deben ser cambiados al menos una vez cada seis meses.

✓Todas las contraseñas de usuario como usuario de equipo, cuentas de email, cuentas de servicios web y cuentas de cliente en aplicaciones deben ser cambiadas al menos una vez cada 60 días.

11.3.10 Política de seguridad de las comunicaciones.

➢**Objetivo:** definir los lineamientos que deben seguirse para asegurar las comunicaciones y sus respectivos mecanismos con el fin de proteger la información de SISELCOM S.A.S.

➢ **Directrices:**

✓La gestión de los dispositivos de red debe realizarse si estos los permiten a través de protocolos seguros (Ej. SSH, IPSEC, SSL, etc.).

✓Deben establecerse controles para proteger el intercambio de Información que SISELCOM S.A.S. pueda realizar como parte de sus actividades de negocio, a través de cualquier canal de comunicación.

✓Se deben realizar conjuntamente tareas de concienciación y capacitación para que los usuarios sean conscientes sobre los riesgos a los que se pueden ver expuestos cuando se realiza intercambios de información, así como también los controles asociados para la protección de la información. Llevando control del mismo en el formato SSC_004 relacionado en el Anexo D.

11.3.11 Política de adquisición, desarrollo y mantenimiento de sistemas.

➢**Objetivo:** asegurar la información que se transmite en la adquisición, desarrollo y mantenimiento de sistemas y activos de información de SISELCOM S.A.S.

➢**Directrices:**

✓Durante los procesos de levantamiento de requerimientos para cualquier sistema o nuevo proyecto, debe contemplarse el diseño e implementación de controles de seguridad.

✓Antes de ser adquiridos productos y/o servicios deben establecerse un proceso formal de pruebas, evaluación y adquisición para garantizar que los servicios y/o productos a adquirir cumplan los estándares, políticas y lineamientos de seguridad de la empresa.

11.3.12 Política de relaciones con los proveedores.

➢**Objetivo:** establecer las directrices en cuando al aseguramiento de las relaciones de los proveedores que tienen relación con SISELCOM S.A.S.

➢**Directrices:**

✓Antes de realizar cualquier tipo de conexión con terceros, debe realizarse un análisis de los riesgos inherentes a la conexión, con el fin de identificar los controles a ser implementados para minimizar el impacto de los mismos.

✓Toda conexión nueva hacia redes de terceros debe pasar a través de una revisión de seguridad. Estas revisiones se realizan para garantizar que todos los accesos coincidan con los requerimientos del negocio.

✓Debe establecerse acuerdos de intercambio de información y software entre SISELCOM S.A.S. y cualquier tercero con el cual se requiera realizar este proceso. Estos intercambios en algunos casos son parte del acuerdo contractual firmado entre las partes.

11.3.13 Gestión de incidentes de seguridad de la información.

➢**Objetivo:** establecer los lineamientos en cuando al reporte y tratamiento de incidentes de seguridad en SISELCOM S.A.S.

➢**Directrices:**

✓Es responsabilidad de cada trabajador de SISELCOM S.A.S., contratista, consultor o tercero, reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas y lineamientos de seguridad a través de los medios establecidos local y corporativamente.

✓Cada vez que se evidencie claramente que SISELCOM S.A.S. ha sido víctima de un delito informático, una investigación forense debe ser ejecutada. Las

investigaciones deben proveer la información suficiente para que la gerencia pueda ejecutar los pasos requeridos para garantizar que el evento no pueda presentarse nuevamente y que las medidas de seguridad asociadas vuelvan a ser restablecidas.

✓Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a la gerencia de SISELCOM S.A.S.

11.3.14 Continuidad del negocio.

➢**Objetivo:** establecer los lineamientos para la continuidad del negocio en SISELCOM S.A.S.

➢**Directrices:**

✓Debe establecerse las medidas de seguridad necesarias para garantizar que la Información que pudiese almacenarse por requerimientos del negocio se encuentre libre de software malicioso.

✓Debe establecerse los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo solo lo pueda realizar personal debidamente autorizado.

✓Todos los funcionarios de la compañía son responsables de los respaldos de la información siguiendo las indicaciones técnicas dictadas por esta política.

11.3.15 Cumplimiento. Los diferentes aspectos contemplados en esta política son de obligatorio cumplimiento para todos los funcionarios, contratistas y otros colaboradores de SISELCOM S.A.S. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, se tomará las acciones disciplinarias y legales correspondientes.

11.4 ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD

Teniendo en cuenta la evolución que tiene la tecnología y las amenazas de seguridad que se evidencian día a día, y en cumplimiento con los requerimientos legales que se encuentren vigentes aplicables a la empresa y al sistema de gestión de seguridad de la información, la gerencia de SISELCOM S.A.S. se reserva el derecho a modificar esta política cuando se necesario. Esta política será revisada con regularidad como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados, realizando revisiones anuales de la misma. Los cambios realizados en esta política serán divulgados a todos los

usuarios de la empresa. Es responsabilidad de cada uno de los usuarios la lectura y conocimiento dela política de seguridad más reciente.

12. PLAN DE FORMACIÓN Y CONCIENCIACIÓN

Hoy, más del 85% de los ataques provienen desde el interior de las propias empresas (empleados descontentos, fraude interno, accesos no autorizados, falta de motivación) y, a través de la ingeniería social. Esto se debe a que resulta más fácil obtener la contraseña de un usuario en la red de las empresas, que vulnerar los sistemas de seguridad y cifrado.

"Muchas instituciones no prestan la suficiente atención a su recurso humano, que puede llegar a ser el eslabón más débil en la cadena de la seguridad de la información, por lo que es necesario sensibilizarlos o capacitarlos sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información"[19].

Realizar un plan de sensibilización y capacitación dentro de una empresa, es fundamental para la creación de un modelo de atención de incidentes y requerimientos de seguridad, por tal motivo cada vez son más las empresas que invierten en programas de capacitación para sus empleados, con el fin de aumentar la productividad y generar ventajas competitivas que lleven a un mejor posicionamiento en el mercado. La capacitación empresarial promueve el aprendizaje en determinadas áreas del conocimiento y fortalece las habilidades de los empleados para alcanzar un ejercicio profesional más óptimo.

➢¿Porque necesitamos un plan de sensibilización en seguridad de la información?

✓Existe la mentalidad que no hay nada importante por proteger en su computador.

✓Existe el concepto errado que la tecnología por si misma puede resolver sus problemas de seguridad.

✓Continuamente se generan nuevos métodos de "Ingeniería Social" que mediante engaños buscan obtener información confidencial.

✓No se tiene el de las amenazas externas como las internas.

Debido a todas estas razones, el plan de sensibilización para el nuevo modelo de seguridad de la información para la SISELCOM, es lograr que las personas conozcan los motivos y razones que generan los diferentes tipos de incidentes en seguridad de la información que existen alrededor de cada uno y acojan las

[19] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Plan Comunicación Sensibilización. [en línea]. Bogotá: MinTC, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

debidas precauciones recomendadas a través medios de concienciación y sensibilización.

12.1 DESCRIPCIÓN DEL PLAN DE FORMACIÓN Y CONCIENCIACIÓN

Un programa efectivo de formación y concienciación en seguridad de la información debe explicar de manera apropiada las reglas de comportamiento y uso de los sistemas (hardware y software), la información que se maneja al interior de la empresa, lo que se encuentra plasmado en la política de seguridad de la empresa y requiere que sea cumplido por parte de todos los usuarios ya sea contratistas o personal directo.

En el texto anterior, un plan de sensibilización y capacitación adecuado, dentro de la empresa se debe llevar a cabo con base a las siguientes alternativas que se recomiendan utilizar para que el plan de sensibilización sea factible.

- Folletos.
- Uso de tecnología.
- Presentaciones de capacitación.
- Carteles

La campaña de sensibilización dentro de la empresa está desarrollada al personal directo de la empresa como a personal colaborador externo, evidenciando que es un grupo pequeño tendrá una duración mínima de seis (6) meses, que iniciarán con el plan de sensibilización y presentación de políticas de seguridad de la empresa, y después, se desarrollará un apoyo por medio de folletos y en equipos de la empresa fondos de pantalla y foros en internet para dar a conocer masivamente el desarrollo de las capacitaciones. Lo anterior teniendo en cuenta que el personal se encuentra en campo y en diferentes ciudades.

12.2 TIEMPO ESTIMADO DE SENSIBILIZACIÓN

La campaña de sensibilización y capacitación al personal que labora de manera directa con la empresa, como el personal contratista, tendrá una duración mínima de seis (6) meses, que iniciarán con el plan de sensibilización, cursos en las instalaciones de la empresa, cada uno con una intensidad de 2 horas quincenales y se tendrá el apoyo por medio de los afiches, fondos de pantalla y folletos para dar a conocer masivamente la campaña y generar conciencia en cada uno de los participantes e integrantes de la empresa.

En cuanto a los folletos, se recomienda entregarlos al ingreso de la empresa, se desarrollará el proceso a todos los visitantes, empleados y contratistas, creando un compromiso y un impacto positivo, garantizando que la información va llegar directamente y no a esperas de la capacitación.

12.3 FINANCIAMIENTO DEL PLAN DE FORMACIÓN

En un plan de formación y sensibilización para la empresa SISELCOM, ha destinado un rubro específico para esta labor en el presupuesto anual del 2018, los cuales se distribuyen de la siguiente manera.

- Material de capacitación (papelería).
- Refrigerios para el personal.
- Costo capacitador (Personal que imparte la capacitación).

Para los posteriores procesos de formación, se tiene programado diseñar e implementar los fondos de pantalla propuestos para ser instalados en los computadores de los funcionarios, este es el medio de contacto más directo para crear conciencia de la seguridad de la información, valiéndose de elementos visuales que servirán principalmente para sensibilizar y reforzar los principios básicos de la seguridad de la información. El costo de este diseño sería muy mínimo, casi que nulo ya que internet se encuentra un sin número de páginas que permiten descargar el contenido referente a la protección de la información y de los datos.

12.4 MATERIAL DE CAPACITACIÓN (PAPELERÍA)

Es importante diferenciar que un material de sensibilización y capacitación no debe tener el mismo grado de complejidad que un material de entrenamiento, ya que el entrenamiento busca que el usuario después de ser entrenado adquiera unas habilidades específicas para sus labores, mientras que el material de sensibilización busca disuadir a los usuarios a comportarse de determinada manera, para evitar consecuencias tanto para él, como para la empresa.

Dentro del proceso de capacitación se debe tener en cuenta que existen unos gastos asociados a papelería que estarían destinados de la siguiente manera, es de tener en cuenta que el proceso inicial seria para el personal de planta y tres contratistas el procedimiento que se toma para siete (7) personas.

12.5 DESARROLLO DE MATERIAL PARA SENSIBILIZACIÓN

Es indispensable ratificar que el proceso de sensibilización es algo que aplicará para toda la empresa por igual. Todos los empleados y personal comprometido con la información deben ver el proceso de sensibilización y capacitación como una responsabilidad compartida en seguridad de la información y que todos son importantes en esa labor.

Entre los temas más importantes de sensibilización se encuentran los siguientes:

- Administración de contraseñas.

- Uso y manejo de inventario.
- Software permitido y prohibido en los equipos de la empresa.
- Uso de dispositivos de la entidad fuera de las instalaciones.
- Uso de correo electrónico e identificación de correos sospechoso.
- Identificación de correos sospechosos.
- Seguridad en el puesto de trabajo.
- Ingeniería social.
- Backup y recuperación.
- Amenazas y vulnerabilidades comunes.
- Roles y responsabilidades en la entidad.
- Delitos informáticos
- Seguridad Física
- Ingeniería Social

Los anteriores temas deben estar avalados por la alta gerencia, quien es el ente que determina su ejecución.

12.5.1 Afiches. En un proceso de sensibilización y capacitación para la empresa se busca posicionamiento y continuidad visual de la campaña, divulgando los temas del modelo de seguridad de la información básicos para la empresa.

Los afiches se colocarán al inicio de "la campaña de sensibilización dando a conocer lo que se quiere hacer para que las personas se familiaricen con el nuevo modelo de seguridad de la información"[20]; la idea es que se cambien cada mes con nuevos enunciados para que las personas tengan en cuenta las principales prevenciones, peligros y factores relacionados con la seguridad de la información.

A continuación, se explican los afiches propuestos para la campaña:

[20] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Plan Comunicación Sensibilización. [en línea]. Bogotá: MinTC, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

Figura 38. Afiche Recordatorio

Fuente. El Autores

En la Figura 38 se muestra el afiche diseñado para recordar a las personas, de una manera diferente, que deben cerrar la sesión de su computador cuando no se encuentren en el puesto de trabajo. Esto evitará que personas ajenas realicen acciones no autorizadas o peligrosas desde el mismo.

12.5.2 Fondo de pantalla. El fondo de pantalla es "en ordenadores personales, tabletas y dispositivos de comunicación, la imagen que se utiliza en el fondo de una interfaz gráfica de usuario en una pantalla de ordenador y un dispositivo móvil"[21]. Este sistema permite a las empresas realizar un recordatorio o comunicados importantes a los diferentes usuarios, este método de sensibilización es más efectivo.

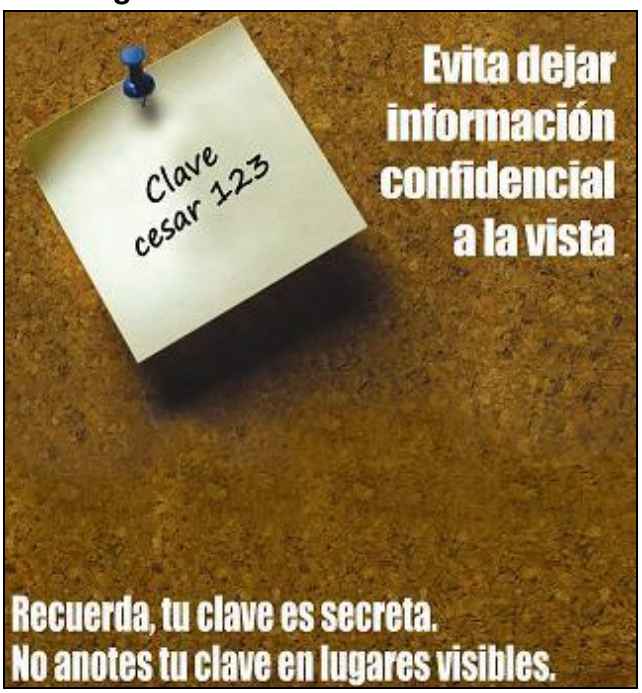
[21] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Plan Comunicación Sensibilización. [en línea]. Bogotá: MinTC, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

Figura 39. Bloqueo equipo

Fuente. Los Autores

En el afiche mostrado en la Figura 39 se quiere transmitir a las personas lo importante que es para la empresa o para ellas mismas, la información que poseen en su computador. Se quiere llamar, de una manera diferente, la atención y curiosidad de las personas.

Figura 40. Contraseña segura



Fuente. Los Autores

El afiche de la Figura 40 quiere dar a conocer de una forma gráfica a las personas, los errores en que generalmente incurren con su información personal; con esto se

trata de sensibilizar sobre los principales factores de la seguridad de la información como son la confidencialidad, la integridad y la disponibilidad.

12.5.3 Folletos. Es una de las herramientas que ofrece información masiva más detallada sobre los aspectos más relevantes del modelo de seguridad que cuenta la empresa. Los folletos serán distribuidos al mismo tiempo que se lancen los primeros afiches de la campaña, con esto se le da apoyo y un impacto más proporcionado.

Es indispensable ratificar que el proceso de sensibilización mediante la entrega de folletos en la cual se debe tener en cuenta los temas a tratar en las capacitaciones, brindando un preámbulo y un proceso dinámico a la vista de todos que intervienen en el proceso de sensibilización.

Entre los temas más importantes de sensibilización se encuentran los siguientes:

- Administración de contraseñas.
- Uso y manejo de inventario.
- Software permitido y prohibido en los equipos de la empresa.
- Uso de dispositivos de la entidad fuera de las instalaciones.
- Uso de correo electrónico e identificación de correos sospechoso.
- Identificación de correos sospechosos.
- Seguridad en el puesto de trabajo.
- Ingeniería social.
- Backup y recuperación.
- Amenazas y vulnerabilidades comunes.
- Roles y responsabilidades en la entidad.
- Delitos informáticos
- Seguridad Física
- Ingeniería Social

El proceso de diseño de cada folleto correo por cuenta de la empresa y del personal que sea designado a esta labor, ya que requiere una serie de gastos, que el proceso de gestión del presente proyecto no se tiene presente.

13. CONCLUSIONES

Al realizar el diseño del sistema de gestión de seguridad de la información bajo la norma ISO 27001:2013 para la empresa SISELCOM S.A.S, se logró establecer el estado actual de cumplimiento frente a la norma, encontrando que la empresa se encuentra en la primera etapa de madurez de cumplimiento ya que en la empresa nunca había tenido en cuenta la seguridad en sus procesos y no se tenían conocimientos sobre el tema, esto se evidencio en las encuestas realizadas a la gerencia y a los empleados donde en la mayoría de los casos se obtuvieron respuestas negativas en cuanto a conocimiento y cumplimiento de los controles de la norma.

En el levantamiento de información se realizaron visitas de campo y encuestas al personal directo de la empresa con preguntas relacionadas con sus procesos y por el tamaño de la empresa se realizó una encuesta personalizada a la gerencia que es la que cuenta con toda la información del manejo de los procesos y así obtener el estado real del manejo de los procesos y de la seguridad.

El análisis de riesgo se realizó tomando en cuenta las necesidades del negocio ya que en el momento para la empresa de acuerdo a su línea de negocio se da más importancia al cuidado y mantenimiento de activos, en este análisis encontramos que el 8% de los activos se encuentra en un riesgo alto que se tiene que tratar lo antes posible y la mayoría de activos que equivalen a un 46% se encuentran en un estado riesgoso y corresponden en su mayoría a los equipos que la empresa tiene en alquiler como núcleo del negocio por lo que se debe dar prioridad.

Dentro del plan de aplicabilidad para dar tratamiento a los controles incumplidos que representan un riesgo alto para la empresa se encontró que para remediar estos riesgos no se necesita una inversión muy alta con algunos ajustes en su esquema de seguridad, documentación y capacitación se pueden remediar estos riesgos que pueden representar un mayor costo para la empresa a futuro si no se da un tratamiento inmediato.

El análisis de cada uno de los hallazgos encontrados es uno de los objetivos más importantes, ya que la seguridad de la información normalmente se relaciona a temas de ataques informáticos pero con este proyecto se logró evidenciar que la seguridad de la información en realidad es un conjunto de componentes como son las personas, la tecnología, el ambiente, la política, las normativas o reglamentaciones donde todos los procesos de la empresa ayuden a gestionar adecuadamente la información y esto permitió identificar las causas, efectos y recomendaciones para la empresa.

14. RECOMENDACIONES

La empresa actualmente se encuentra en un porcentaje de cumplimiento frente a la norma del 11%, el estado deseado que la empresa quiere alcanzar inicialmente es del 80% por lo que se realizan las siguientes recomendaciones para alcanzar este indicador.

Inicialmente se recomienda a la empresa establecer, implementar y mantener un sistema de gestión de la calidad que este alineado con los objetivos y planes estratégicos de negocio de acuerdo con la norma ISO 9001:2015 e incluya un compromiso de mejora continua del sistema de gestión de la calidad. Al implementar este sistema se terminarán de documentar todos los procedimientos y políticas lo que ayudaría a aumentar el porcentaje de cumplimiento de la norma ISO 27001:2013 en aproximadamente un 12% ya que de los 114 controles en nuestro concepto 14 se podrían cumplir con un adecuado sistema de gestión de calidad.

Se recomienda a SISELCOM S.A.S. implementar la política de seguridad diseñada en el presente proyecto y realizar las actualizaciones o adecuaciones necesarias cuando se presenten cambios relevantes, con esta adecuada implementación se espera aumentar el cumplimiento frente a la norma del 53% ya que bajo nuestro concepto 60 controles podrían cumplirse al implementar esta política.

Finalmente es necesario que la empresa implemente los planes de mitigación recomendados para reducir las amenazas encontradas dentro del análisis de riesgo con esta implementación se espera que el porcentaje de cumplimiento del 10% que incluyen 11 controles de la norma.

Al implementar estas recomendaciones se espera que la empresa logre un nivel de cumplimiento frente a la norma del 86%.

BIBLIOGRAFÍA

27001ACADEMY. Listado de documentación requerida ISO-27001:2013 [en línea]. Bogotá: Wordpress, 2014 [fecha de consulta 5 de octubre de 2017]. Disponible en: https://lciso27000.files.wordpress.com/2015/02/iso-27001-lista-documentacion-requerida.pdf

ANGE, Camilo. ¿Qué es un activo de información?. [en línea]. Bogotá: Wordpress, 2010 [fecha de consulta: 15 de octubre de 2017]. Disponible en: https://camiloangel.wordpress.com/2010/09/03/ %c2%bfque-es-un-activo-de-informacion/

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES. Glosario. [en línea]. Bogotá: Ministerio de las TIC, 2015 [fecha de consulta: 15 de octubre de 2017]. Disponible en: www.mintic.gov.co/gestionti/615/articles-6099_recurso_2.docx › General

-------. Plan Comunicación Sensibilización. [en línea]. Bogotá: MinTC, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: https://www.mintic.gov.co /gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

CONSEJO SUPERIOR UNIVERSITARIO. Acuerdo 046 (1 de diciembre de 2009). Por el cual se definen y aprueban las políticas de Informática y Comunicaciones que se aplicarán en la Universidad Nacional de Colombia. Bogotá: Universidad Nacional de Colombia, 2009. p. 1

CORNEJO, M.; GARCÍA, M.; GONZÁLEZ, I.M. y GUERRERO, M.N. Principios de Seguridad Informática en Sistemas de Información. [en línea]. México: Universidad Autónoma del Estado de Hidalgo, 2015 [fecha de consulta 5 de octubre de 2017]. Disponible en: https://www.uaeh.edu.mx /scige/boletin/tlahuelilpan/n6/e5.html

ESCUELA DE ADMINISTRACIÓN, FINANZAS Y TECNOLOGÍA. ¿Qué son medidas de tratamiento. [en línea]. Medellin: EAFIT, 2010 [fecha de consulta: 25 de abril de 2016]. Disponible en: www.eafit.edu.co/.../Nota%20de%20Clase% 2010%20Medidas%20de%20Tratamiento

GUTIÉRREZ AMAYA, Camilo. Análisis de riesgos. [en línea]. Buenos Aires: Welive Security, 2012 [fecha de consulta: 15 de octubre de 2017]. Disponible en: www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

GYJ SECURITY CONSULTING GROUP. Seguridad en personas. [en línea]. Bogotá: G&J Group, 2017 [fecha de consulta 7 de agosto de 2017]. Disponible en: http://gyjgroup.com/seguridad-personas.html

HIDALGO LÓPEZ, Celvin Manolo. La firma electrónica avanzada y su certificación. Guatemala: Universidad de San Carlos, 2014. p. 101

ICONTEC INTERNACIONAL. Sistema de gestión de seguridad de la información. [en línea]. Bogotá: ICONTEC, 2010 [fecha de consulta 5 de octubre de 2017]. Disponible en: http://www.icontec.org/Ser/Ed/Paginas/Sgsi.aspx

INSTITUTO CARO Y CUERVO. ¿Qué es política de seguridad?. [en línea]. Bogotá: Instituto Caro y Cuerto, 2010 [fecha de consulta: 25 de abril de 2016]. Disponible en: www.caroycuervo.gov.co/ sites/.../POLÍTICA% 20DE%20 SEGURIDAD% 20ICC_0.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACION ICONTEC. Sistema de gestión de seguridad de la información. [en línea]. Bogotá: ICONTEC, 2013 [fecha de consulta 5 de octubre de 2017]. Disponible en: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf

-------. Documentación. Presentación de tesis, trabajos de grado y otros trabajos de investigación. NTC 1486. Sexta actualización. Bogotá: ICONTEC, 2008. 36 p.

INSTITUTO ESPAÑOL DE ANALISTAS. ¿Qué es control?. [en línea]. Madrid: IEAF, 2013 [fecha de consulta: 15 de octubre de 2017]. Disponible en: ieaf.es/new/lideres-de.../control-y...riesgos.../1561-que-es-el-control-de-riesgos.html

ISOTOOLS EXCELLENCE. ISO 27001: ¿Qué significa la Seguridad de la Información?. [en línea]. Bogotá: ISO Tools, 2015 [fecha de consulta 5 de octubre de 2017]. Disponible en: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

MERCADO LIBRE. Muebles para Oficinas Vitrinas Comerciales. [en línea]. Bogotá: Mercado Libre, 2017 [fecha de consulta 7agosto de 2017]. Disponible en: http://articulo.mercadolibre.com.co/MCO-445587912-shelving-estanteria-stocker-en-metal-y-madera-de-200x18-hct2-_JM

PORTAL ISO 9001. Procedimientos documentados. [en línea]. Bogotá: ISO, 2014 [fecha de consulta 14 de octubre de 2017]. Disponible en: http://iso9001calidad.com/introduccion-procedimientos-147.html

REVISO. ¿Qué es un activo?. [en línea]. Bogotá: Reviso, 2016 [fecha de consulta: 15 de octubre de 2017]. Disponible en: https://www.reviso.com/es/que-es-un-activo

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO UNAM. Esquemas de Seguridad Informática. [en Línea]. México: UNAM, 2014 [fecha de consulta 7 de marzo de 2017]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php

WORDPRESS. ¿Qué es un activo de información? [en línea]. Bogotá: Wordpress, 2010 [fecha de consulta 15 de octubre de 2017]. Disponible en: https://camiloangel.wordpress.com/2010/09/03/%c2%bfque-es-un-activo-de-informacion/

WORDPRESS. Ciclo de mejora continua PHVA [en línea]. Bogotá: Blog – Top, 2007 [fecha de consulta 5 de octubre de 2017]. Disponible en: http://www.blog-top.com/el-ciclo-phva-planear-hacer-verificar-actuar/

ANEXOS

Anexo A. Reporte Pérdida de Equipos o Información

SISELCOM Sistemas Eléctricos y de Comunicaciones S.A.S. **REPORTE PÉRDIDA DE EQUIPOS O INFORMACIÓN**			
Formato: SSC_002			
REPORTE No.:		FECHA:	
TIPO DE PÉRDIDA:			
EQUIPO:		INFORMACIÓN:	
DESCRIPCIÓN DE INCIDENTE:			
DATOS DEL EQUIPO O INFORMACIÓN:			
UBICACIÓN:			
RESPONSABLE:			
OBSERVACIONES:			
FIRMA RESPONSABLE:			
CÉDULA:			

Anexo B. Autorización para Entrada y Salida de Materiales y/o Equipos

SISTEMAS ELÉCTRICOS DE COMUNICACIONES S.A.S.
AUTORIZACIÓN PARA ENTRADA Y SALIDA DE MATERIALES y/o EQUIPOS

Formato: SSC_001

Se Autoriza a:				**C.C.:**
Retirar:		**Ingresar:**		
Contratista:				
En el Vehículo de Placas:				
Destino:		**Empresa:**		

Cant.	**Descripción**	**Marca**	**Serie**	**Modelo**

Observaciones: (Período o tiempo de salida autorizado):

Autorizado Por:					
Nombre y Firma de Quine Recibe \ Entrega:					
Lugar y Fecha:		**Hora Entrada:**		**Hora Salida:**	

Anexo C. Acta de Entrega Individual de Activos e Inventarios a Funcionarios y/o Contratistas

ACTA DE ENTREGA INDIVIDUAL DE ACTIVOS E INVENTARIOS A FUNCIONARIOS y/o CONTRATISTAS

Formato: SSC_003

Ciudad y Fecha: _____

Por medio de la presente, se hace entrega formal de los siguientes activos:

Descripción del activo	Serial no.	Marca	Modelo	Estado

Observaciones:

_____

_____

Cláusula de Compromiso: Como funcionario de Siselcom declaro que los activos relacionados en el presente documento están bajo mi responsabilidad, por lo cual les daré un uso adecuado al desempeño de mis funciones y a la destinación institucional prevista para cada uno de ellos. En consecuencia, serán asumidos por mí el daño o la pérdida de los mismos debidos a mi negligencia o incumplimiento de las instrucciones relacionados con su uso y conservación. Me comprometo a informar oportunamente a la gerencia sobre cualquier desplazamiento, siniestro, reparación, traslado, reintegro, cambio de responsable temporal o definitivo, y sobre cualquier situación que ponga en inminente riesgo los bienes de la empresa.

FIRMA QUIEN ENTREGA EL ACTIVO
Nombre:
Identificación:
Cargo:

FIRMA QUIEN RECIBE EL ACTIVO
Nombre:
Identificación:
Cargo:

Anexo D. Listado de Asistencia

SISTEMAS ELÉCTRICOS DE COMUNICACIONES S.A.S.
LISTADO DE ASISTENCIA

Formato: SSC_004
Ciudad y Fecha: _____

Nombre de la Formación	
Nombre del formador:	
Objetivo:	
Contenidos:	

No.	Nombres y Apellidos	No. Cedula	Firma
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Autorización uso de información personal: con la firma del presente documento, el asistente a esta formación autoriza en forma expresa a Siselcom, para que de manera responsable haga uso de los datos de carácter personal que se encuentren en la bases de datos de Siselcom o que se obtengan legítimamente con ocasión de esta formación.